NASA/TM-2005-213750/Version 1.0
NESC-RP-05-18

Space Shuttle Orbiter Reaction Jet Driver (RJD)

Independent Technical Assessment/Inspection (ITA/I) Report

Richard J. Gilbrech
NASA Langley Research Center, Hampton, Virginia

Robert A. Kichak, Mitchell Davis, Glenn Williams, and Walter Thomas III
Goddard Space Flight Center, Greenbelt, Maryland

George A. Slenski
Wright-Patterson Air Force Base, Ohio

Mark Hetzel
Jet Propulsion Laboratory, Pasadena, California

March 2005

NASA/TM-2005-213750/Version 1.0
NESC-RP-05-18

Space Shuttle Orbiter Reaction Jet Driver (RJD)

Independent Technical Assessment/Inspection (ITA/I) Report

Richard J. Gilbrech
NASA Langley Research Center, Hampton, Virginia

Robert A. Kichak, Mitchell Davis, Glenn Williams, and Walter Thomas III
Goddard Space Flight Center, Greenbelt, Maryland

George A. Slenski
Wright-Patterson Air Force Base, Ohio

Mark Hetzel
Jet Propulsion Laboratory, Pasadena, California

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

March 2005

The use of trademarks or names of manufacturers in the report is for accurate reporting and does not constitute an official endorsement, either expressed or implied, of such products or manufacturers by the National Aeronautics and Space Administration.

Available from:

NASA Center for AeroSpace Information (CASI)
7121 Standard Drive
Hanover, MD 21076-1320
(301) 621-0390

National Technical Information Service (NTIS)
5285 Port Royal Road
Springfield, VA 22161-2171
(703) 605-6000

Space Shuttle Orbiter Reaction Jet Driver (RJD)

Independent Technical Assessment/Inspection (ITA/I)

Report

Performed and Prepared by

The NASA Engineering and Safety Center (NESC)

March 22, 2005

VOLUME I: ITA/I REPORT

TABLE OF CONTENTS

1.0 AUTHORIZATION AND NOTIFICATION 4

2.0 SIGNATURE PAGE (ASSESSMENT TEAM MEMBERS) 5

3.0 TEAM MEMBERS AND CONSULTANTS 6

4.0 EXECUTIVE SUMMARY 7

5.0 OVERVIEW OF INITIAL ITA/I PLAN 9

6.0 PROBLEM, PROPOSED SOLUTIONS, RISK ASSESSMENT 9
6.1 Problem 9
6.2 Technical Description 9
6.3 Proposed Solutions 11
6.4 Risk Assessments 11

7.0 DATA ANALYSIS 12
7.1 Results of Tests and Analyses 12
7.1.1 Orbiter Project Proposed Solution 12
7.2 Risk Mitigations 12
7.2.1 Wire Short Risk Mitigation 12
7.2.2 Darlington Pair Risk Mitigation 14
7.2.3 Pin-to-Pin Short Risk Mitigation 14
7.3 NESC PRA Evaluation 15
7.3.1 NESC Evaluation of Ames Wire-to-Wire Short PRA 15
7.3.2 NESC Evaluation of SAIC's PRA 17
7.4 NESC Independent Evaluation Approach 19
7.4.1 Wire-to-Wire "Smart" Short Evaluation Approach 19
7.4.2 Darlington Transistor Evaluation Approach 21
7.4.2.1 Analyses 21
7.4.2.2 Pre-Flight Leakage Current Testing 25
7.4.2.3 Destructive Physical Analysis 28
7.4.2.4 Data Search 28
7.5 NESC Independent PRA 28
7.5.1 RJD Wire-To-Wire "Smart" Short Failure Mode 29
7.5.2 Darlington Pair Failure Mode 30
7.5.3 Recommendations on Improving NESC PRA Estimates for Wire-to-Wire "Smart" Short Failure Mode 32

8.0 FINDINGS, OBSERVATIONS and RECOMMENDATIONS 34
8.1 Findings from KSC Site Inspection 34
8.2 Observations 35
8.3 Recommendations 37

9.0 REFERENCES 39
10.0 LIST OF ACRONYMS 40
11.0 MINORITY REPORT (dissenting opinions) 42
12.0 LESSONS LEARNED 42

List of Figures

6.2-1 Five Root Causes of Inadvertent Thruster Firing 10
7.2.3-1 Back Shell Short vVia Wire Braid Strand, Metal Chip Contamination Considered Remote Due to Connector "Cork And Bottle" Interfacial Seal 15
7.3.1-1 Crow-AMSAA Plot of STS Orbiter Interconnect Short Circuits 16
7.3.2-1 Typical Failure Distribution Functions 18
7.4.1-1 Orbiter RJD Wiring Schematic 20
7.4.2.1-1 Example of PSPICE RJD Drive Circuit Simulation Model 22
7.4.2.1-2 Darlington Transistor Failure Mode Tree 24
7.4.2.1-3 Comparison of Transistor Safe Operating Area and Fuse Characteristic 25
7.4.2.2-1 Leakage Current Measurement Location Options 26
7.4.2.2-2 Q1 leakage Current vs. Thruster Coil Current 27
7.5.1-1 Wire-to-Wire "Smart" Short Aggregated Failure Probability for 28 Flights 30
7.5.2-1 Darlington Transistor Aggregated Failure Probability for 28 Flights 31
7.5.2-2 Darlington Transistor Failure Analysis History 32
8.1-1 Orbiter Cables with Unsupported Lengths 34
8.1-2 Teflon-insulated wires contacting sharp corners within the RJD box 35

VOLUME II: APPENDICES

A. RJD Illustrations
B. Consolidated Failure Mode Listing
C. PRA of Failures Leading to the Inadvertent Firing of Thrusters While the Orbiter is Docked to the International Space Station
D. Darlington Transistor Test Plan
E. RJD Shielded Wire Dry Arc-Track Test
F. Aerospace Darlington Transistor Assessment Report
G. Wiring Damage Analyses for STS OV-103
H. Team Member Biographies

Volume I: ITA/I Report

1.0 AUTHORIZATION AND NOTIFICATION

The Space Shuttle Program (SSP) has a zero-fault-tolerant design related to an inadvertent firing of the primary reaction control jets on the Orbiter during mated operations with the International Space Station (ISS). Failure modes identified by the program as a wire-to-wire "smart" short or a Darlington transistor short resulting in a failed-on primary thruster during mated operations with ISS can drive forces that exceed the structural capabilities of the docked Shuttle/ISS structure. Mr. Bryan O'Connor, NASA's Chief Safety and Mission Assurance (S&MA) Officer, initiated an assessment on April 19, 2004, by requesting the NESC to review the issue and render a technical opinion on the probability of a catastrophic failure related to this scenario. Other stakeholders include Mr. William Parsons, the SSP Manager, and Mr. William Gerstenmaier, the ISS Program Manager. The SSP liaison assigned is Mr. Donald Totton, Deputy Manager, SSP S&MA.

The ITA/I Plan was developed by Dr. Richard Gilbrech and approved by the NESC Review Board (NRB) on June 18, 2004. The scope of the ITA/I was a combination of review and independent analyses that included:

1. Review of statistical methods and assumptions for wire-to-wire "smart" short and Darlington transistor pair failure Probabilistic Risk Assessments (PRAs) conducted by the Program.
2. Evaluation of Darlington pair wear-out mechanisms, wire-short-related mechanisms, corresponding program mitigations, and pros/cons of redesigned RJD avionics.
3. Development of a NESC position on failure probability estimates.
4. Recommendation as appropriate of any risk mitigation that the program has not considered or independent testing that could reduce uncertainty in risk predictions.

The ITA/I lead and the NESC Director briefed Mr. O'Connor at NASA Headquarters on August 25, 2004, along with the SSP and ISS stakeholders (vehicle, engineering and S&MA management representatives from both Programs) on the preliminary results of the assessment. Inputs from this meeting were incorporated into subsequent briefs to the SSP Integration Control Board on September 28, 2004, the SSP Program Requirements Control Board (PRCB) on September 30, 2004, and the SSP/ISS Joint PRCB on October 4, 2004.

2.0 SIGNATURE PAGE (ASSESSMENT TEAM MEMBERS)

Dr. Richard Gilbrech, NASA/LaRC NESC Principal Engineer	Robert Kichak, NASA/GSFC NESC Avionics Discipline Expert
Mitchell Davis, NASA/GSFC	Glenn Williams, NASA/GRC
Walter Thomas, NASA/GSFC	George Slenski, WPAFB
Mark Hetzel, NASA/JPL	

3.0 TEAM MEMBERS AND CONSULTANTS

Team Members

Dr. Richard Gilbrech	NESC Principal Engineer, Lead	NASA/LaRC
Robert Kichak	NESC Avionics Discipline Expert	NASA/GSFC
Mitchell Davis	Avionics	NASA/GSFC
Glenn Williams	Avionics	NASA/GRC
Walter Thomas	Reliability Engineer	NASA/GSFC
George Slenski	Wiring	WPAFB
Mark Hetzel	Wiring	NASA/JPL
Pam Fullen	Program Analyst	NASA/LaRC

Consultants

Dr. Daniel Schrage	Professor	Georgia Tech
Dr. Vitali Volovoi	Research Engineer	Georgia Tech
Tim Wilson	NESC KSC Chief Engineer	NASA/LaRC
Tom Draus	OMS/RCS System Lead	NASA KSC
Dr. Henning Leidecker	Avionics	NASA/GSFC
Edward (Ted) Kopf	Avionics	NASA/JPL
Lanny Plaisance	Wiring	NASA/JSC
Hung Nguyen	Wiring	NASA/KSC
Michael Stirling	Wiring	NASA/KSC
Rob Cherny	Electrical	Orbital Sciences
Steve Battel	Electrical	Battel Engineering
Daniel Yuchnovicz	NESC Systems Engineer	NASA/LaRC
Dr. Terry St. Clair	Polyimide Materials	Consultant

4.0 EXECUTIVE SUMMARY

The SSP has recognized that a zero-fault-tolerant design related to an inadvertent firing of the primary reaction control system (RCS) jets exists on the Orbiter during mated operations with the ISS. There are 44 RCS thrusters on each Orbiter, 38 primary thrusters (870 lbf thrust each) and 6 vernier thrusters (24 lbf thrust each). ISS loads analysis has shown limit load exceedances of structural interfaces and solar array assemblies from an inadvertent primary thruster firing. The loads exceedances increase in severity as the moment of inertia of ISS increases toward complete assembly. Catastrophic failure for both SSP and ISS would likely result from those loads exceedances.

The SSP requires critical systems to be "fail ops/fail safe," or dual fault tolerant. In the past, effective mitigation strategies for the zero-fault-tolerant RJD have included removal of power from the RJD box when the function is not required, and a provision for manual RCS propellant manifold shutdown by the crew, if necessary. RJD power is also removed during extravehicular activity (EVA) and during the majority of ground operations when personnel are in proximity to a fueled Orbiter. The RJD is powered on for a short period (~18 hours) during flight turnaround ground processing to perform the RJD functional check, with access limited to essential personnel only.

This assessment addressed three of the identified root causes of an inadvertent primary thruster firing: failure (fail short) of the RJD Darlington pair transistor switch, a wire-to-wire "smart" short in the RJD wiring bundle between a hot (powered) wire and a thruster command wire, and a pin-to-pin short (hot) in the RJD connectors. A pin-to-pin short could occur either between two thruster command pins resulting in two jets firing instead of the one selected or between a power pin and a command pin where the jet would fire inadvertently. The Shuttle Program determined a range of probabilities related to the wire-to-wire "smart" short (1.4 x 10^{-4} to 6.4 x 10^{-8}) per flight and an estimate of the RJD Darlington pair failure probability (9.5 x 10^{-8}) per flight. The pin-to-pin short was deemed remote and NESC concurred with the Program's accepted risk rationale.

Specifically placed outside the scope of this assessment were two other inadvertent firing failure modes identified by the Program: multiplexer/demultiplexer (MDM) erroneous output and general purpose computer (GPC) erroneous output. These were judged by the Program to be improbable. A software modification has been approved and is being implemented by the Program for the next two flights. This will automatically close the RCS propellant manifold feeding the failed-on thruster if an inadvertent firing is sensed during mated Shuttle/ISS operations. The modification will limit the inadvertent thruster firing duration to less than 1.5 seconds that, according to analysis conducted by the Program, will prevent exceeding structural limits. Review of this software modification was also purposefully placed outside the scope of this assessment.

Several risk mitigation options for the wire-to-wire "smart" short and Darlington pair failure modes were considered by the SSP ranging from replacing RJD wire with new shielded cable to redesigning the RJD avionics box with high-side/low-side switching. The Orbiter Program recommended the high-side/low-side switching option for implementation at the April 15, 2004, Space Shuttle PRCB. This option eliminates the risk from both Darlington pairs and wire-to-wire "smart" shorts. The first ship set of redesigned RJDs would be delivered for installation in 25 months after authority to proceed with an estimated cost of $29M. The new high-side/low-side switching would provide single-fault-tolerance to failure modes that could result in inadvertent thruster firing. The propellant manifold auto-close software modification is claimed to only be effective for the next two flights. After these two flights (Space Transportation System (STS) STS-114/LF1 and STS-121/ULF1.1), the Programs would have to accept the risk of a catastrophic inadvertent thruster firing for at least six flights (STS-115/12A to STS-120/10A). The RJD fix would then be in effect for the 22 remaining ISS assembly missions starting with STS-122. The SSP Manager's decision was to not implement this modification and discuss the issue at the Joint Shuttle/ISS PRCB.

NESC concluded that the current Critical Items List (CIL) waiver rationale is not adequate since it does not consider aging effects for 25+ year old parts; does not capture all credible failure modes; and there is a near-instantaneous nature of failure while docked, rendering mitigating actions of the crew ineffective.

The assessment team delivered 17 observations, 6 findings and 15 recommendations to the SSP. The majority of the technical team and over half of the NRB recommended that the RJD box high-side/low-side switch redesign commence immediately. However, the NESC ultimately recommended replacing the RJD wire with new, better-protected wiring, conducting Darlington electrical and destructive physical analysis (DPA) tests and adding pre-flight leakage current tests by no later than STS-115/12A. After evaluating that data, NESC will deliver a recommendation on the RJD box high-side/low-side switch redesign. Risk exists that negative results could drive the redesign to be a constraint. Also, a delayed start of a redesign effort would expand exposure until the upgraded RJD is installed. The NESC observed that for scenarios having relatively low probability of failure on a single flight, for multiple flights the probability of failure accumulates directly according to the number of flights, i.e., 20 times greater for 20 flights than for a single flight. An action plan addressing the 15 NESC recommendations was requested and is in work by the SSP.

5.0 OVERVIEW OF INITIAL ITA/I PLAN

The scope of the RJD assessment included a combination of review, independent analyses, and tests as follows:

1. Evaluation of the failure modes and assessment of possibilities. This included identifying any stresses acting on the wire and Darlington transistors.
2. Review of statistical methods and assumptions for wire-short-related failures and Darlington pair failure PRAs conducted by the Program.
3. Evaluation of Darlington pair wear-out mechanisms, wire-short-related mechanisms, and corresponding program mitigations.
4. Recommendation of any program risk mitigations not considered or independent testing that could reduce uncertainty in risk predictions.

Specifically placed outside the scope of the ITA/I Plan, completed in June 2004, were risks posed by the other three failure modes identified by the Program that would result in an inadvertent primary reaction jet firing (connector pin-to-pin shorts, MDM erroneous output, and GPC erroneous output) and the effectiveness of the software modification to automatically detect a failed-on thruster and close the corresponding reaction jet propellant manifold. Note that over the course of the review, sufficient data was provided for the NESC to concur with the Program's accepted risk rationale for the connector pin-to-pin short.

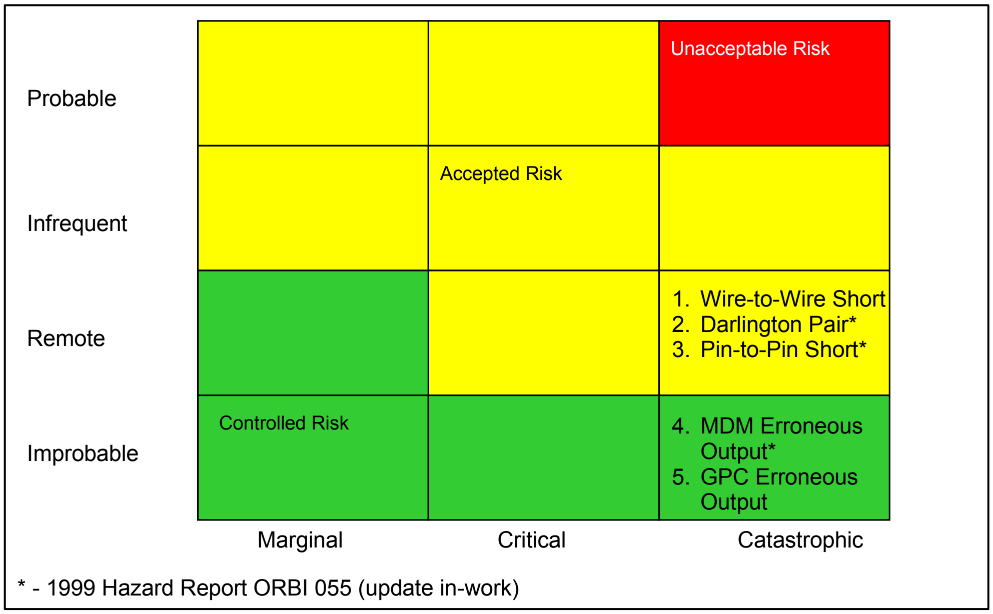
6.0 PROBLEM, PROPOSED SOLUTIONS, RISK ASSESSMENT

6.1 Problem

Failure modes which result in a failed-on primary thruster drive forces during mated operations with ISS that can exceed the structural capabilities of the docked Shuttle/ISS structure. The RCS thrusters are assigned to four RJD boxes on the Orbiter: 2 fwd and 2 aft — each thruster having its own driver.

6.2 Technical Description

The primary focus of this assessment included a wire-to-wire "smart" short of a powered wire to a valve solenoid wire and any RJD Darlington pair transistor failing short. Figure 6.2-1 illustrates five potential root causes for inadvertent thrusting and the Program's risk assessment of them.



	Marginal	Critical	Catastrophic
Probable			Unacceptable Risk
Infrequent		Accepted Risk	
Remote			1. Wire-to-Wire Short 2. Darlington Pair* 3. Pin-to-Pin Short*
Improbable	Controlled Risk		4. MDM Erroneous Output* 5. GPC Erroneous Output

* - 1999 Hazard Report ORBI 055 (update in-work)

Figure 6.2-1. Five Root Causes of Inadvertent Thruster Firing

a. Consequences from National Space Transportation System (NSTS) 22254:

- **Catastrophic**: Hazard could result in a mishap resulting in fatal injury to personnel and/or loss of one or more major elements of the flight vehicle or ground facility.
- **Critical**: Hazard could result in serious injury to personnel and/or damage to flight or ground equipment which would cause mission abort or a significant program delay.
- **Marginal**: Hazard could result in a mishap of minor nature inflicting first-aid injury to personnel and/or damage to flight or ground equipment which can be tolerated without abort or repaired without significant delay.

b. Likelihoods based on NSTS 07700-10-Master Verification Plan (MVP)-01:

- **Probable**: Will occur several times in the life of the Program. A general guideline for likelihood of occurrence would be 1 in 12 to 125 flights ($8 \times 10^{-2} > X > 8 \times 10^{-3}$).
- **Infrequent**: Likely to occur sometime in the life of the Program. A general guideline for likelihood of occurrence would be 1 in 125 to 1,250 flights ($8 \times 10^{-3} > X > 8 \times 10^{-4}$).
- **Remote**: Unlikely, but possible, to occur in the life of the Program. A general guideline for likelihood of occurrence would be 1 in 1,250 to 12,500 flights ($8 \times 10^{-4} > X > 8 \times 10^{-5}$).

- **Improbable**: So unlikely that it can be assumed occurrence may not be experienced in the life of the Program. A general guideline for likelihood of occurrence would be greater than 1 in 12,500 flights ($X < 8 \times 10^{-5}$).

6.3 Proposed Solutions

Proposed solutions include identifying all failure modes resulting in inadvertent firing, evaluating the failure modes and then assessing the probabilities. These include identifying any stresses acting on the wire and Darlington transistors, and reviewing statistical methods and assumptions used by the Program for wire-short-related failures and Darlington pair failure PRAs. An independent, dynamic PRA via fault tree analysis will then be developed and anchored with independent analysis and testing. Recommendations, as appropriate, will be made for any program risk mitigations not considered or independent testing that could reduce uncertainty in risk predictions.

6.4 Risk Assessments

Mr. Bryan O'Connor, NASA's Chief S&MA Officer, requested a review and independent PRA on April 19, 2004. The NESC PRA, located in Volume II, Appendix C of this report, was conducted by Dr. Vitali V. Volovoi [6] (as part of the ITA/I) to quantify and describe the risks of failures leading to the inadvertent firing of thrusters while the Orbiter is docked to the ISS. Risk mitigations are also discussed in Section 7.2 of this report.

7.0 DATA ANALYSIS

7.1 Results of Tests and Analyses

7.1.1 Orbiter Project Proposed Solution

The Orbiter Project's proposed solution was to modify the RJD with high-side and low-side switching which would be effective for *both* the wire-to-wire "smart" short and Darlington pair failure modes. In addition to the design changes in the RJD avionics box, this would involve a minor wiring mod at the first bulkhead connector in the wiring chain from the thruster valve toward the RJD to implement the low side return. Due to the time required for implementation, the Orbiter considered accepting risk for 6 flights to include STS-115/12A to STS-120/10A. The RJD fix would then be effective for the 22 remaining flights starting with STS-122. The SSP Manager's decision was to not implement this modification and discuss the issue at the Joint Shuttle/ISS PRCB.

7.2 Risk Mitigations

This section will discuss the Program's risk mitigations for the wire-to-wire "smart" short, the Darlington pair failure, and the connector pin-to-pin short. Note that while the pin-to-pin short was originally placed outside the scope of the assessment, over the course of the review sufficient data was provided for the NESC to concur with the Program's accepted risk rationale on this hazard. Modeling was developed to examine the wire-to-wire "smart" short and its evolution of wire damage as a function of time. The model allows for the estimation of significant wire damage for a given Orbiter and flight. Relevant significant damage included damaged and exposed conductors. Appendix C of this report provides more detail.

7.2.1 Wire Short Risk Mitigation

Three approaches were used by the Program to estimate the probability of an inadvertent thruster firing caused by a wire-to-wire "smart" short:

1. ***System reliability approach relies on decomposing the catastrophic event into a set of more elementary events and conditions.*** If the relative timing of these events is irrelevant to the occurrence of the catastrophic event, fault trees or Bayesian (belief) networks can be used. Otherwise, a dynamic framework such as Stochastic Petri nets can provide a more accurate description of the probability of occurrence. The main disadvantage of this "white box" approach is that a relatively large number of statistical parameters must be provided to characterize elementary events and conditions as well as their interactions. There is a positive side in that these elementary events are usually less unique than the system as a whole, and as a result, the required parameters can be inferred from the experience gained from other systems and environmental conditions. This approach was taken by the risk assessment conducted by Koushik Datta (NASA

Ames). Some of the assumptions used in that study were questionable, and the resulting point estimate was dismissed as overly conservative by the Shuttle Program.

2. ***Observed reliability approach is based solely on past experience of the system under consideration.*** With this method, the issues of (external) similarities with other systems are avoided; however, due to the scarcity of system-specific data, selecting events that are significantly similar to the studied catastrophic event is challenging. A relatively loose similarity definition poses the problem of accounting for dissimilarity (such as between wire-to-wire vs. wire-to-ground shorts) that is effectively equivalent to the need for event decomposition (see item 1 above). Then again, a more strict definition of similarity leads to a small sampling pool, with resulting difficulties for any meaningful statistical inference. This latter approach was selected by the Shuttle Program as the most credible. Several deficiencies of this approach provide grounds for doubting the resulting numbers.

3. ***Observed reliability approach can be complemented by incorporating external data via the Bayesian approach.*** While theoretically this approach provides a means to compensate for the lack of system-specific data, the final results are very sensitive to the external data, and the construction of a good prior estimate is crucial. This, however, presents a formidable challenge due to the complexity and multitude of confounding factors that make the “black box” comparison of catastrophic events all but impossible. Samandar Roshan-Zamir (Science Applications International Corp. (SAIC)) used this approach by constructing a prior estimate based on civil transport aircraft data. The results do not inspire high confidence, as they provide prior failure rates that are almost two magnitudes lower than the Shuttle-specific data. It is reasonable to suggest that rates, if anything, could be higher (due to less-strict aircraft maintenance practices and the harsher environment seen by aircraft wiring). This Bayesian approach was abandoned in a recent SAIC updated report in lieu of the observed reliability approach described in item 2 above. The final estimate of wire-to-wire “smart” short probability was 9.8×10^{-6}.

The intensive wiring inspection performed after STS-93 corrected many wiring defects and instituted a rigorous plan for inspection, technician training, and wire damage awareness. All accessible wiring gets external visual and tactile inspection (Category 2) during Orbiter Major Maintenance (OMM).

To provide abrasion protection for the wiring, the pan head offset cruciform screws near the harnesses are being replaced with socket-head cap screws. Teflon tape was applied to the wire bundles at the RJD connector backshell tang area. Teflon tape wrap and convolute were added to the harness bundles at high abrasion areas as well as adding Teflon sheet and silicone rubber edging to protect wire bundles at chafe points.

Ground processing tests were used as screens for wire damage (e.g., insulation resistance and Hi-Pot for repaired wire/connectors, functional checkout of wire/connectors before every vehicle flight).

7.2.2 Darlington Pair Risk Mitigation

Hazard Report (HR) ORBI-055, Rationale for Acceptance of Darlington risk, was evaluated as a part of the NESC ITA/I. The HR notes that the RJD transistors are adequately de-rated for both current and voltage and exceed the Orbiter Project Parts List (OPPL) requirements of MF0004-400. The RJD assemblies are qualification (vibration, shock, and temperature) and acceptance-tested (thermal and vibration) to certify the design and to meet operational performance requirements. The RJDs are certified for a life of 10,000 hours, which the HR equates to 100 missions. The RJD also incorporates a Built In Test Equipment (BITE) circuit to indicate jet command ON vs. OFF status. Pre-launch procedures require the Launch Control Center (LCC) to monitor RJD driver power on event telemetry after driver power activation and to monitor jet chamber pressure for any indication of unwanted jet firings. Integrated subsystem verifications are performed during ground turnaround maintenance to ensure proper commands (A & B from the MDM for RJD activation), logic, driver, and trickle current measurements. Note that a shorted jet driver will cause the BITE output to assert a status telemetry point to the MDM.

Samandar Roshan-Zamir (SAIC) used a PRISM® electronic parts reliability database to predict Darlington failure rates. The final Darlington failure rate prediction based on this analysis was 7.15×10^{-9}.

7.2.3 Pin-to-Pin Short Risk Mitigation

Standard controls such as visual inspection of connector mating faces, verifying the plug coupling ring clicks into place, and electrical checkout are sufficient to mitigate these risks. The design practice calls for pin-to-pin short hazard analysis on all Critical 1 functions and separation of command and power pins within a connector. All connector mates are Shuttle Connector Analysis Network (SCAN) tracked, which means that all copper paths, including connector pins, are verified prior to the flight. Bent pins would be detected by this test. The connectors are capped during maintenance and inspected before mating. Finally, a short via shield wire braid debris was considered remote due to the connector “cork and bottle” interfacial seal. Refer to Figure 7.2.3-1.

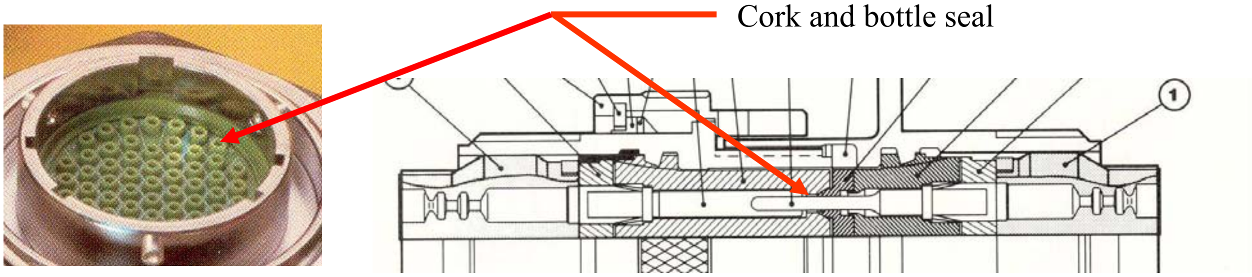


Figure 7.2.3-1. Back Shell Short via Wire Braid Strand, Metal Chip Contamination Considered Remote Due to Connector "Cork and Bottle" Interfacial Seal

7.3 NESC PRA Evaluation

7.3.1 NESC Evaluation of Ames Wire-to-Wire Short PRA

A system level approach was used in the Ames PRA with a Fault Tree (FT) constructed to evaluate the influence of several failure modes. While the study was quite detailed, only a few key assumptions were identified that could be sufficient for obtaining the final numerical results. Namely, wire chafing and carbonization of wires via arc tracking were major contributors to the FT top event, where the top event number was proportional to the number of significant wire damages found during the 1999 OV-102 wire inspections. It was assumed that there was no damage on the initial wire installation, with linearly accumulated damage over 26 flights, and that the 1999 inspections detected and repaired 100% of significant wire damage. No wire aging effects were factored into the analysis (i.e., a Homogeneous Poisson Process (HPP) was used). It was also assumed that the combination of better inspections and less induced damage resulted in a 6-fold reduction of wire failures after 1999. Timing of the wire short was not considered, even though only 9% of total powered time is during the docked window.

Note, the Ames study was considered too conservative, which was the reason it was dismissed by the Shuttle Program. However, some interesting features of this analysis can be examined:

Initially, it was assumed that there was no damage to wires, and this damage uniformly accumulated during 26 flights. This damage was then assumed to be 100% detected during the 1999 inspection. In addition to the issue of detectability, the model does not account for regular maintenance. The difficulty with the approach is the need to reconcile the issues of repairable versus non-repairable systems. A HPP is defined for repairable systems. While HPP assumes that the rate of *accumulated damage* is constant and not the *total amount of damage*, in reality the former is proportional to the latter. Applicability of a HPP implies that each occurring failure is repaired, and the system is restored to its original configuration, i.e., the old damage is removed. With over 150 miles of wiring in the Shuttle, this is equivalent to stating that the overall state of the Shuttle wires neither degrades nor improves with time in any appreciable manner. The state of wires is measured by the frequency of occurrence of the wire damage (that is how many wires are damaged at any point in time).

There were no distinctions made as to when during the turn-around cycle a failure occurs. An assumption that the damage is permanent and immediately detected leads to a simple calculation of a correction factor by dividing the docking time by the total power-on time during one cycle.

Finally, a post-1999 six-fold improvement in the rates of damage requires further justification, as existing data fails to support such an improvement. Moreover, preliminary results from an independent NESC review and analysis of wiring damage data by Walter Thomas indicate that the no-aging assumption might be optimistic as well.

Orbiter short circuit data (collected by P. Krause/Boeing) was analyzed by plotting "all interconnect" short circuit events and wiring short circuit events (a subset of all short circuit events) using the Crow-Army Material Systems Analysis Activity (Crow-AMSAA or CA) [7] model. The time axis used was the "report date", since no details about operating times at event occurrences were available. This is not limiting, since degradation modes can operate exclusive of powered-on times. The results are shown in Figure 7.3.1-1.

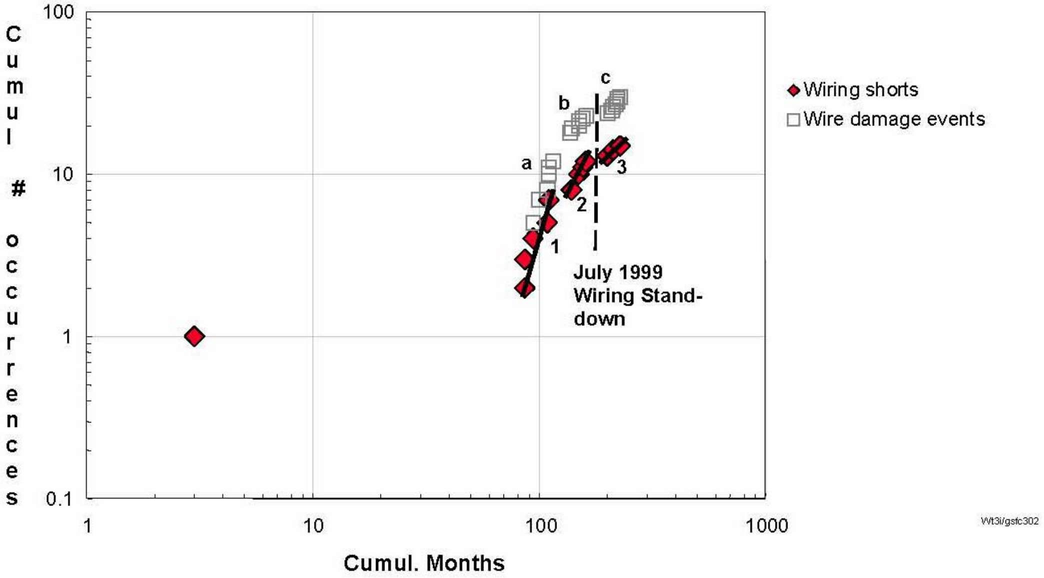


Figure 7.3.1-1. Crow-AMSAA Plot of STS Orbiter Interconnect Short Circuits

The Orbiter wiring short data indicate that wiring shorts may be worsening with time. These data suggest that wire degradation does exist in the Orbiter. More detailed analyses should be performed to confirm details about failure modes and character. Refer to Appendix G of this report.

7.3.2 NESC Evaluation of SAIC's PRA

The PRA was generated by Samandar Roshan-Zamir (SAIC) around January 2004 and then updated in May 2004 with wire-to-wire "smart" short probability of 9.8 x 10^{-6} and Darlington failure of 7.15 x 10^{-9}.

Significant observations include:

- The wire-to-wire short point estimate was based on two prior wire-to-wire shorts (STS-6 humidity separator B in-flight failure and post STS-65 OMM failure of a caution and warning test).
- The PRISM® electronic parts reliability database was used for Darlington failures. Using PRISM® and the MIL-HDBK-217 was outside the scope of the PRA. They are meant to either be a design trade tool or to estimate warranty costs or service intervals—not an absolute source for field (in-service) failure predictions. Tools such as these are intended for predicting average, rather than worst case behavior. The issue is depicted in Figure 7.3.2-1 below.
- The PRA for Darlingtons uses the "Reliability Analysis Center (RAC) Failure Mode/Mechanism Distributions, 1997" collector-to-emitter short only (<0.1%) while the same table shows a normal distribution of "shorted" as 30%. Two of three short modes (collector-to-base, collector-to emitter) are catastrophic and typical of "shorted" condition. This implies that the overall result should be at least x100 higher (more if aging is borne out by tests).
- An earlier version (1991) of RAC "Failure Mode/Distribution Database" (FMD) shows "Transistor, Bipolar" and "Short" at 73%. This is more applicable since these devices were manufactured in the pre-1990s timeframe.

The issue of the detectability of wire-to-wire shorts (especially intermittent ones) remains an unknown, as it is recognized that all shorts reported in the Problem Resolution and Corrective Action (PRACA) database are due to the observed malfunctioning of some equipment. It is reasonable to assume that some intermittent shorts went unnoticed. However, future occurrences of the same shorts are capable of causing a catastrophic event.

NESC notes that aging was not considered in the SAIC analysis. Therefore, two failures do not provide enough information to support or reject any presence of aging. It is important to recognize that the absence of aging is a non-conservative assumption.

Mean Time to Fail ≠ Time to First Failure

Average Failure Rates DO NOT Capture Atypical Behavior of Manufacturing Problems, Insufficient Screening, or Aging Effects

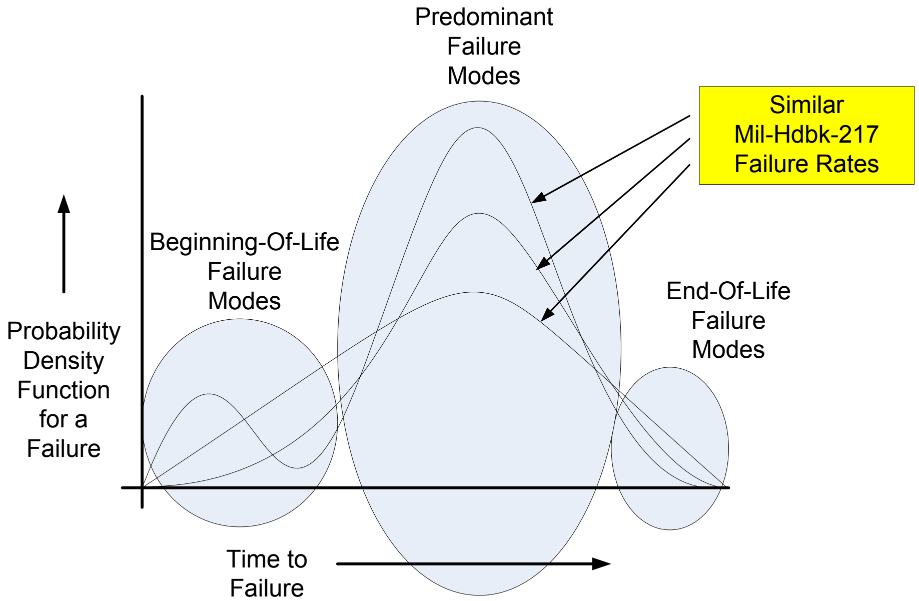

Predominant Failure Modes
Similar Mil-Hdbk-217 Failure Rates
Beginning-Of-Life Failure Modes
End-Of-Life Failure Modes
Probability Density Function for a Failure
Time to Failure

Figure 7.3.2-1. Typical Failure Distribution Functions

- The study accounted for 4,000 feet of RJD control wire, but this is off by a factor of two since another 4,000 feet of wire was necessary to participate in smart short (i.e., 2 x (9.8 x 10^{-6}) = 1.96 x 10^{-5}).

7.4 NESC Independent Evaluation Approach

7.4.1 Wire-to-Wire "Smart" Short Evaluation Approach

The NESC started the investigation into the potential of a wire-to-wire "smart" short in the Orbiter RJD polyimide wiring by examining the KSC failure reports that had been previously generated surrounding two relevant Orbiter wire damage incidents: STS-6 Humidity Separator B tripped 4 circuit breakers due to damaged wiring (OV-099) and the post STS-65 failure of a caution and warning test during OMM (OV-102). Also reviewed were the post-STS-93 wiring tests performed at KSC, the "NASA Orbiter Sampling Test Results and Analysis" Wire Insulation Degradation Analysis System (WIDAS report, N224-RPT16SE0) [9], and the Boeing "New Wire Insulation Study for Potential Orbiter Use" [10], along with other documents.

The NESC visited KSC to take a tour of the Endeavour (OV-105) during an OMM where a large portion of the Orbiter's estimated 150 miles of wiring was exposed. The team noticed that some Orbiter wiring had been insulated in Teflon convolute tubing and marked with yellow tags. It was explained that these wire bundles had been identified as Criticality 1 functions and, therefore, a secondary insulation was placed around them to increase their resistance to mechanical damage and arc track resistance. In the engine compartment area, there were articulating engine gimbals, hydraulic, ammonia, and hydrazine lines, and work platforms that were placed around large engine ducting. There is a small concern regarding fluid leaks onto wiring that may cause a wire short condition. The only fluid present that could rapidly degrade polyimide insulation during a flight is hydrazine. Post-flight inspection is necessary to check for signs of a hydrazine leak. A hydrazine leak would leave telltale signs on painted surfaces and other materials.

A very high percentage of Endeavour's Orbiter wiring received a Category 2 inspection and wire protection modifications. Because of the density of wiring in some areas, it is very hard to inspect wires in the center or back side of bundles without stressing adjacent wiring. Collateral damage of adjacent wiring is why the NESC is recommending abandoning the RJD wiring in place, and adding replacement wiring where space is available. Statistical wire repair data has shown that not all wiring damage is found during inspection or testing, and that a second inspection will sometimes turn up damage that was originally missed. This highlights the difficulty in 100% inspection, and promotes the desire to add fault tolerance to the RJD wiring subsystem. Another concern was in the forward RCS thruster area, where thruster wire insulation showed signs of wear and tear including locations where the color topcoat was missing. Overall, the condition of the wiring looked reasonably good for the age of the Orbiter and its environmental and maintenance exposure. The team visited an area where electrical and mechanical technicians are trained in wiring awareness and repair. This program was instituted after the STS-93 short and subsequent major Orbiter wiring repair effort. Many hands-on wire harness training aids showing "how to" and "how not to" were present. Refer to Appendix A for examples of wire flaws that were presented during a Boeing course. Also, in Appendix A, is a pros/cons chart of the various RJD risk mitigation options that were considered.

During the initial phase of collecting data on the thruster wiring, there was some confusion on what type of wire was used from the RJD boxes to the thrusters. First it was thought to be only single conductor wire. Upon review of the Orbiter wiring schematics, the RJD wire was found to be a mixture of single conductor, twisted pair, twisted shielded pairs and unshielded twisted quads. Also, the thruster wiring is routinely routed with power wires. The wire configuration affects the susceptibility to a smart short or arc track event. Two cable block diagrams highlighting a forward and aft thruster were generated to show the many wire configurations and bulkhead connectors along the path from the RJD boxes to the thrusters. Also, two RJD thruster connector pinouts were diagrammed to show the proximity of power pins to RJD valve coil wires. For the most part, signal separation guidelines are followed, but further investigation is needed on the remaining RJD thruster connectors. A schematic of the RJD wiring configuration, shown in Figure 7.4.1-1, was developed by the NESC from the Orbiter wire database to facilitate analysis.

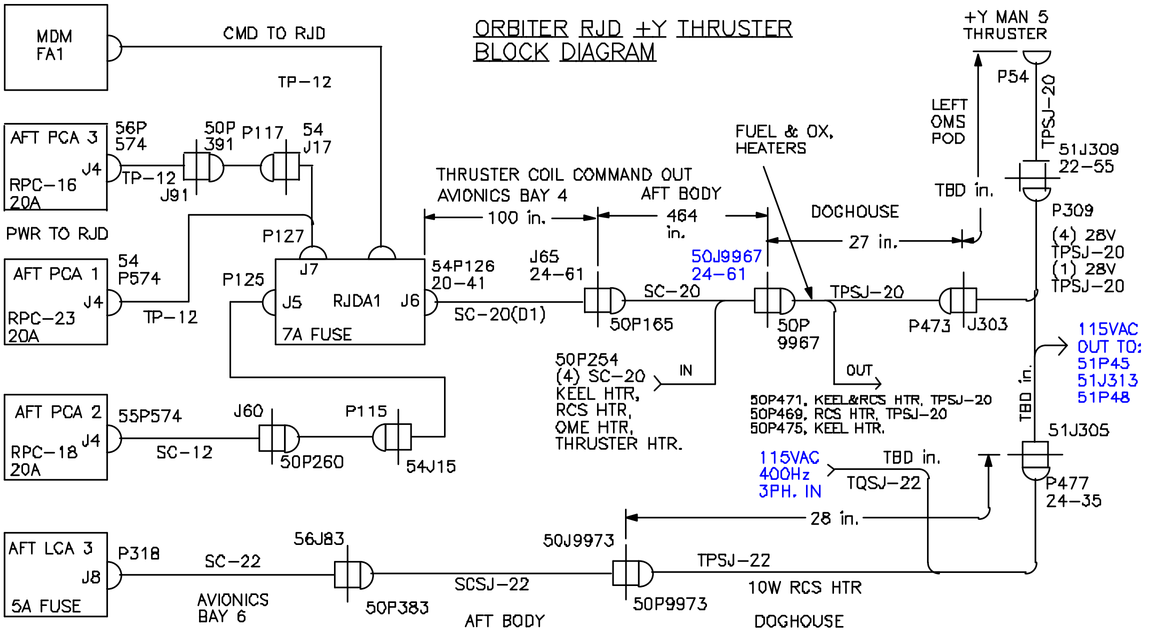


Figure 7.4.1-1. Orbiter RJD Wiring Schematic

The susceptibility of polyimide wire to arc tracking and aging was investigated. An arc track event can occur between a thruster command wire and an adjacent power wire through

1. a wire-to-wire "smart" short;

2. a power wire that arc tracks to structure and is in the same bundle with a RJD valve coil wire; or

3. a power wire arc tracks to a return wire and is in the same bundle with a RJD valve coil wire.

A wealth of information was gained from the post STS-93 wire testing program at KSC and from George Slenski's experience with aircraft wiring problems. Dr. Terry St. Clair, an expert consultant in polyimide, was questioned regarding any aging mechanisms present in the polyimide film and possible test methods to determine degradation. It was concluded that at the present time there is no definitive test available to determine aging effects in polyimide wire insulation. As for arc tracking, it is a well established problem with polyimide wire insulation in certain wire configurations. Polyimide wire was originally selected for its excellent dielectric withstanding voltage, cut-through resistance, and light weight. After the STS-93 incident, the Orbiter Project performed extensive research to find a new wire replacement for the polyimide wire. The conclusion was that polyimide was still the best choice for the Orbiter. The Orbiter Project has protected some Crit 1 functions with Teflon convolute tubing, but the RJD thruster wiring has not been protected in this manner. The NESC proposed wire testing including one to determine the effectiveness of various wire configurations and secondary insulation protections against an arc track event.

In conclusion, it is the NESC team's recommendation to replace the RJD thruster wiring with new polyimide wiring in a configuration determined by the proposed wire testing recommendations. The existing RJD thruster wiring would be abandoned-in-place to minimize damage to the adjacent wiring.

7.4.2 Darlington Transistor Evaluation Approach

7.4.2.1 Analyses

PSPICE modeling of the electrical circuits (typical example shown in Figure 7.4.2.1-1) was used to quantify the circuit parameters of assumed failure modes. Review of WSTF test data indicated that the minimum energy necessary to activate both the fuel and oxidizer thruster valves is 12 VDC at 1A. This was the threshold used in the circuit analysis to determine a jet fire/no-fire outcome. In general, the RJD circuit is a robust design concerning the risk of inadvertent thruster firing. The designers did an excellent job isolating power sources from the critical circuit areas, thus lowering the risk of inadvertent firing due to circuit failures. This is considered an extremely important point if a redesign is considered for the STS or the next generation vehicle. There were numerous model simulation runs (~85) that are not included in the official report since the assumed failure modes were proven to be unrealistic or of no consequence to an inadvertent thruster firing. The following summary will concentrate on the most probable assumed failure modes.

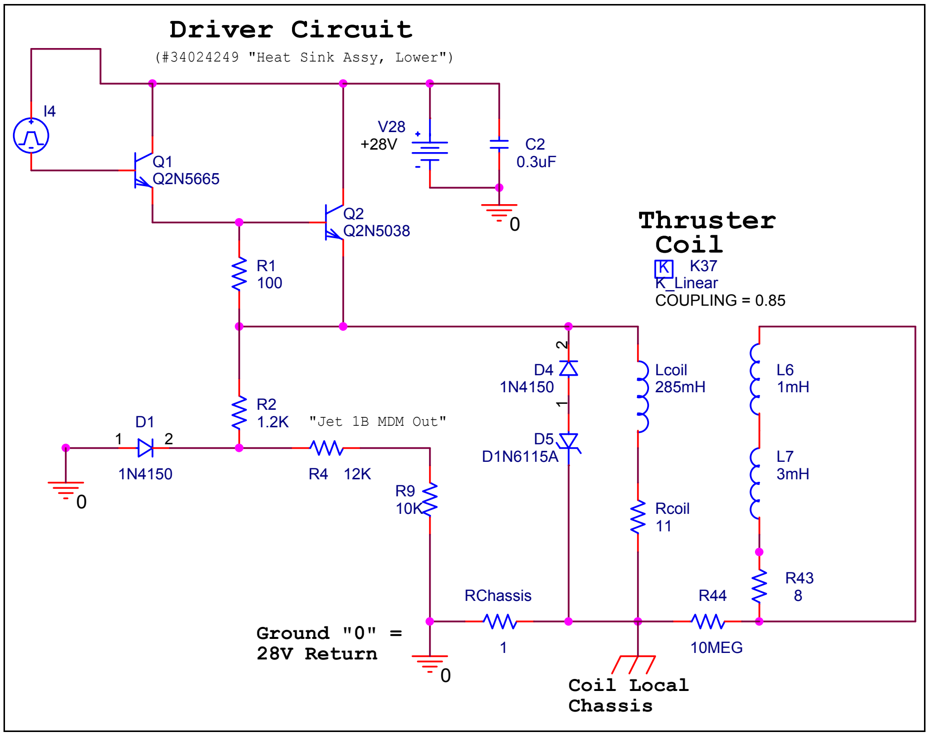


Figure 7.4.2.1-1. Example of PSPICE RJD Drive Circuit Simulation Model

A transistor pair configured as a Darlington Pair controls the thruster activation. For this discussion, the input transistor (2N5682) will be called Q1 and the output transistor (2N5038) will be called Q2. The key to reducing potential failure modes is to isolate all energy sources away from the base of Q1. There are four entry points into the driver circuit plus the single output thruster drive signal. The four are: the “transformer isolated” command input, the MDM telemetry output, a test point (J2-1 TP1) and the 28 VDC power connected to the collector of the Darlington pair. All four of the entry points were investigated as a potential source of energy into the circuit that may cause an inadvertent thruster firing.

The test point was eliminated as a potential energy source after the complete drawing package was received. “J2-1 TP1” actually exists on the printed circuit card on a connector. However, this connector is internal to the assembly and can only be accessed by removing a cover. Thus, this test point was eliminated as a potential failure mode.

The MDM telemetry point connects to the output thruster drive signal through a 12kΩ resistor. Due to this isolation resistor, no realistic MDM circuit failure could deliver sufficient energy to activate the thruster; hence, this input was eliminated as a potential failure mode.

The RJD assembly receives activation commands over several control signals that drive the primary side of a transformer. The secondary side of the transformer is connected directly to the base of Q1. One potential failure mode would be a primary-to-secondary transformer short that would allow a control signal to connect directly into the base of Q1. The modeling indicated that if this short were to occur, the result would be a partial activation of the Darlington Pair. The maximum thruster valve current would be approximately 50mA and, therefore, insufficient energy to activate the thruster valve. This scenario was eliminated as a potential failure mode.

The 28 VDC power connects directly to the collectors of Q1 and Q2; there are no other circuit elements or potential current paths. Therefore, all potential failure modes involve a current path inside either transistor package from the collector to the base. The modeling assumed a collector to base resistive path and that the transistors were otherwise operating nominally. Additionally, to determine the threshold leakage current of one transistor, the other transistor leakage current was set to zero. In reality, the leakage current will be additive and thus the individual minimum shorting resistance may be slightly higher. For Q1, a resistive short between the collector and the base of less than 7kΩ will activate the switch. For Q2, a resistive short between the collector and the base of less than 400Ω will activate the switch. Thus, it does not require a hard short to activate the switch and provide sufficient current to fire the thruster.

Failure modes for the Darlington transistors that could potentially cause thruster firing identified by the NESC are shown in Figure 7.4.2.1-2.

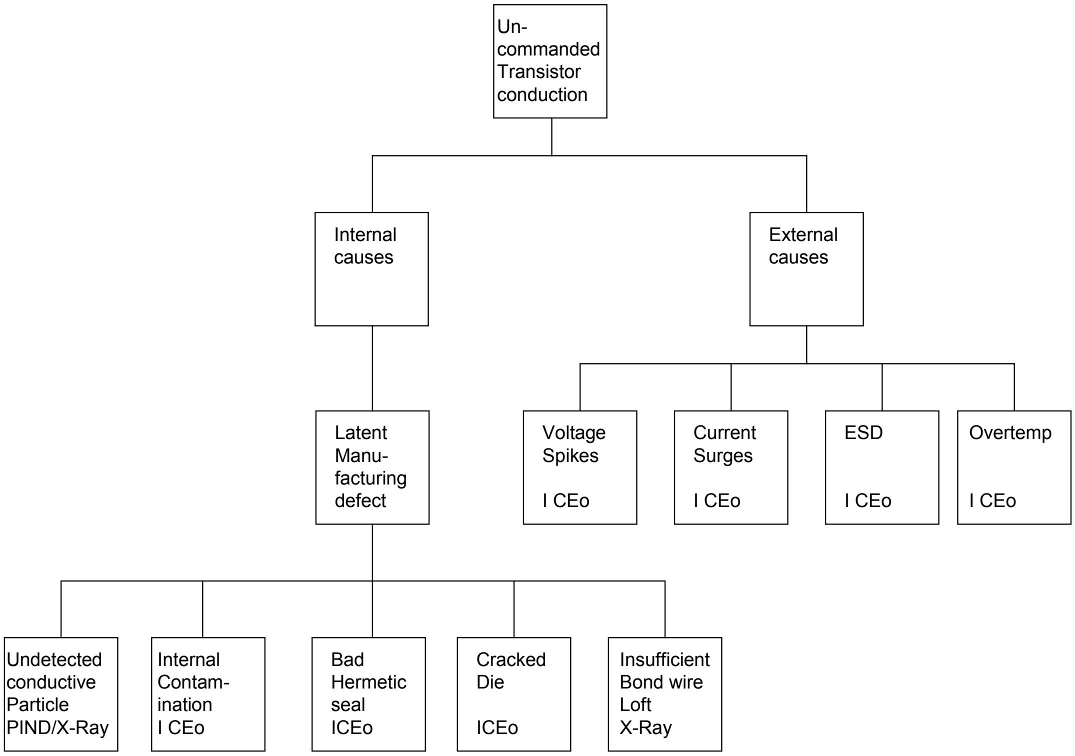

Un-commanded Transistor conduction
Internal causes
External causes
Latent Manu-facturing defect
Voltage Spikes I CEo
Current Surges I CEo
ESD I CEo
Overtemp I CEo
Undetected conductive Particle PIND/X-Ray
Internal Contam-ination I CEo
Bad Hermetic seal ICEo
Cracked Die ICEo
Insufficient Bond wire Loft X-Ray

Figure 7.4.2.1-2. Darlington Transistor Failure Mode Tree

One other feature of the present design is that analysis shows that the Darlington transistor can be damaged by external overloads that increase leakage current or cause a short circuit without opening the fuse in series with it. A comparison of the transistor safe operating area and the fuse characteristic is shown in Figure 7.4.2.1-3 illustrating this concern.

From On Semiconductor Data Sheet for 2N5038

*Indicates JEDEC Registered Data.
(2) Pulse Test: Pulse Width ≤ 300, μs, Duty Cycle ≤ 2%.

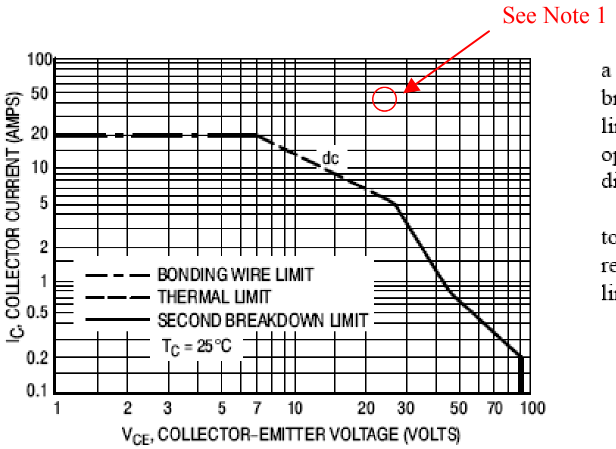


Figure 2. Forward Bias Safe Operating Area

There are two limitations on the power handling ability of a transistor: average junction temperature and second breakdown. Safe operating area curves indicate $I_C - V_{CE}$ limits of the transistor that must be observed for reliable operation; i.e., the transistor must not be subjected to greater dissipation than the curves indicate.

Second breakdown pulse limits are valid for duty cycles to 10%. At high case temperatures, thermal limitations may reduce the power that can be handled to values less than the limitations imposed by second breakdown.

Notes:
1) Red circle on chart is approximate fuse open characteristic for a 300 usec short circuit
2) Transistor drive current may limit short circuit current to a lower value causing transistor short but impeding fuse open

ME451-0010-1070 Fuse Specification (7 A Bussman)	
140.0 Amps	.00010 to .00020 Seconds
45.0 Amps	.002 to .015 Seconds
16.0 Amps	.018 to 3.0 Seconds

Figure 7.4.2.1-3. Comparison of Transistor Safe Operating Area and Fuse Characteristic

7.4.2.2 Pre-Flight Leakage Current Testing

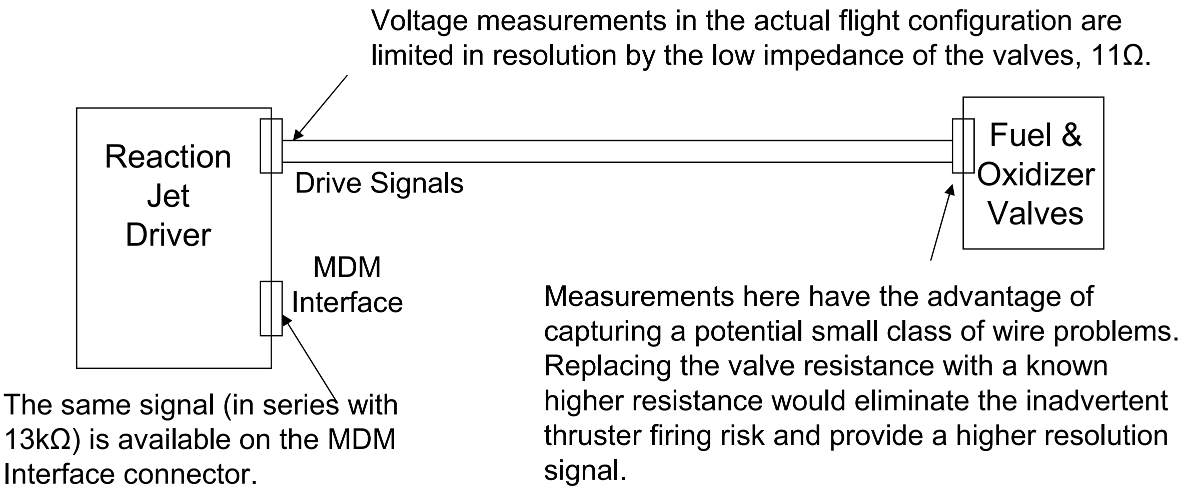
Since it does not require a hard short of the Darlington transistors to fire the thrusters, the NESC has studied and recommended leakage current testing to measure all Darlington pair leakage currents and to verify that they fall within an acceptable distribution. Any Darlington pair measurement that is not “in-family” should be investigated to determine the cause. The data can also be used to trend an individual Darlington pair’s leakage current throughout its lifetime.

This test has the potential to detect seven of nine identified potential failure modes as follows:

1. internal contamination;
2. cracked die;
3. damaged hermetic seal;
4. electrostatic discharge (ESD) damage;
5. current surge;
6. voltage spike; or
7. over temperature latent damage.

It will not identify these potential failure modes: undetected conductive particles inside the transistor package (i.e., Particle Impact Noise Detection Test (PIND) escapes several instances of which have been documented in the Government/Industry Data Exchange Program (GIDEP) as having caused failures on other programs and insufficient bond wire loft).

The exact leakage current and expected distribution of this parameter to the transistor population has not been calculated. However, it should be in the tens of micro-amp range up to milliamp range prior to the final failure. The procedure would be to power on the RJD, but not to command the thrusters to fire. The test would measure voltage across a known resistance to infer the leakage current. The measurement can be made at three locations: the RJD interface, the MDM interface, or the closest available connector to the actual valves. Each location has advantages and disadvantages, which are described in Figure 7.4.2.2-1.



Voltage measurements in the actual flight configuration are limited in resolution by the low impedance of the valves, 11Ω.

Measurements here have the advantage of capturing a potential small class of wire problems. Replacing the valve resistance with a known higher resistance would eliminate the inadvertent thruster firing risk and provide a higher resolution signal.

The same signal (in series with 13kΩ) is available on the MDM Interface connector.

Figure 7.4.2.2-1. Leakage Current Measurement Location Options

The optimal test configuration would be to measure the voltage across a known resistance to infer the leakage current since generally voltage measurements are far easier to accomplish than current measurements. The measurement resolution is determined by (and directly proportional to) the Darlington pair load impedance. Impedance can be selected to provide the desired leakage current measurement resolution. Since the circuit is essentially a current source, one would expect a low-level DC voltage. Any AC characteristics observed during this measurement would be of interest.

Assuming a measurement resolution of 1 mV and a load resistance of 11Ω, then the leakage current resolution would be ~90μA. If the coil was replaced by a 10kΩ load, then the leakage current resolution would be ~0.1μA.

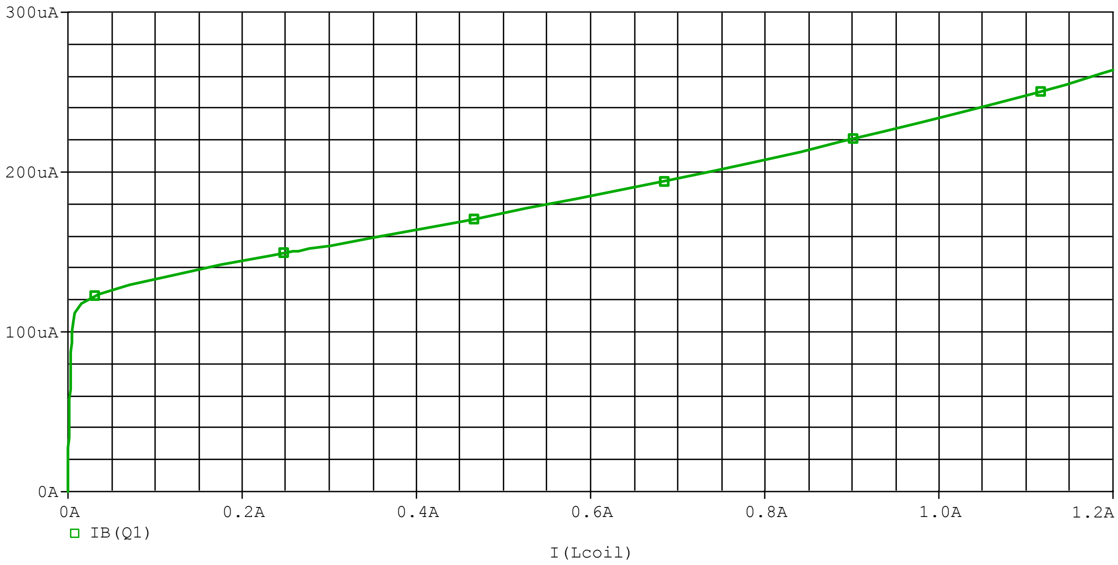


Figure 7.4.2.2-2. Q1 leakage Current vs. Thruster Coil Current

The plot shown in Figure 7.4.2.2-2 indicates the relationship between a potential Q1 (driver transistor) base leakage current and the thruster current. Leakage current from Q2 (output transistor) would have a similar effect only at a different magnitude. The actual box-level measurement will include the base leakage current of Q1 (multiplied by the gain of Q2) plus the base leakage current of Q2.

In summary, this test has the capability to characterize the RJD Darlington pair leakage current for comparison of unit-to-unit as well as one unit over time. A damaged unit will be identified by "out of family" signature prior to a hard failure. Seven of the nine potential Darlington pair failure modes will have a signature of increased leakage current. There is flexibility in the test method and configuration to find that optimal point of maximum knowledge gained at the minimal test-induced risk. Investigation of "out-of-family" units may provide information on currently unidentified failure modes. Finally, the knowledge regarding a potential RJD failure mode changes from a binary state (pass/fail) to an analog level indicating the degree of damage to a unit.

7.4.2.3 Destructive Physical Analysis

The NESC recommends inspections, electrical tests, and DPA of representative samples of the flight Darlington transistors to characterize them and to determine if signs of part deterioration due to aging effects and/or manufacturing defects are present. A second group of parts will also be characterized with regard to electrical overload performance and ESD sensitivity. A test plan is included in Volume II, Appendix D, of this report.

7.4.2.4 Data Search

A search of data on the Darlington transistors has shown that a number of GIDEP alerts exist on some of the manufacturers of these parts types in a number of lot date codes. Flight hardware lot date codes are being researched and data received to date has not shown direct coincidence. PRACA records have also been researched for the RJDs and cases of ground test units having transistor high leakage failures caused by external mis-wiring have been recorded at the White Sands Test Facility (WTSF). This demonstrates that the RJD can be damaged by external faults.

7.5 NESC Independent PRA

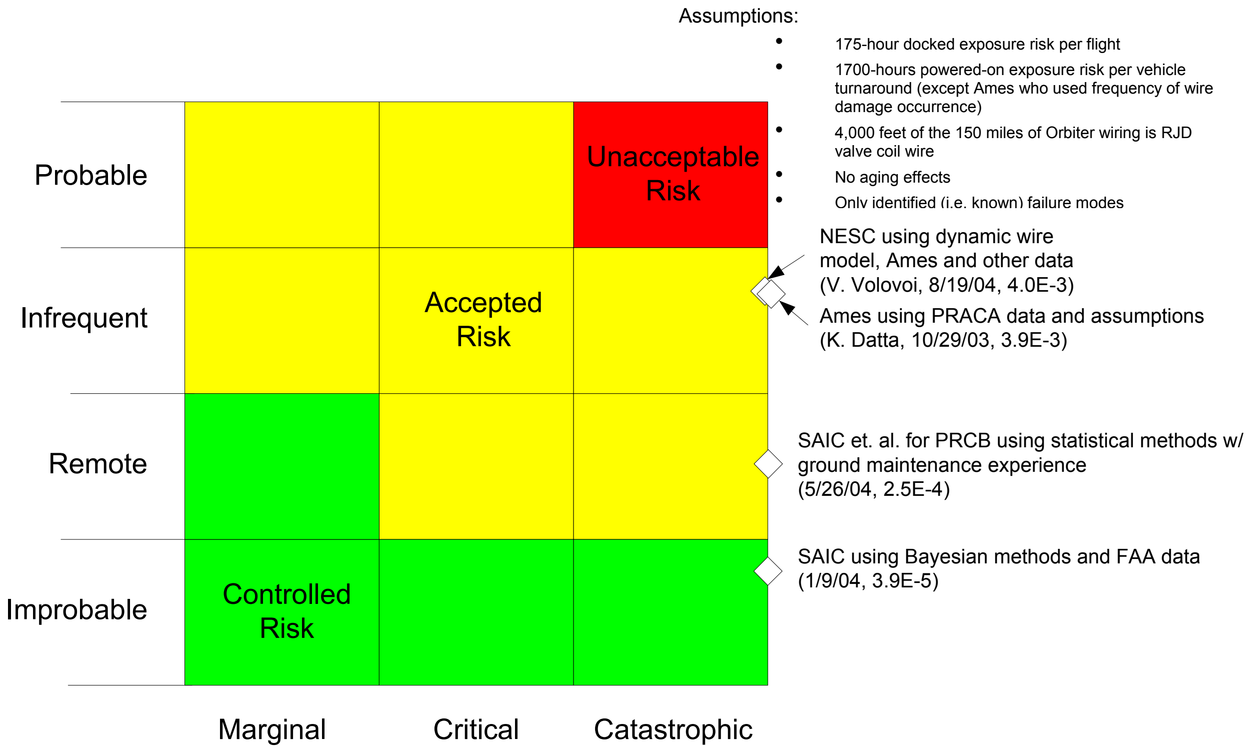
The PRA was generated by Vitali Volovoi (Georgia Tech Research Engineer [6]) with wire-to-wire "smart" short probability for OV-103 of 1.5 x 10^{-4} per flight or ~4 x 10^{-3} for 28 flights and Darlington failure at 1.18 x 10^{-5} per flight or 3 x 10^{-4} for 28 flights. Refer to Appendix C of this report. Aerospace Corporation was tasked by NESC to develop independent probability estimates for the Darlington transistors, using MIL-HDBK-217C and -217F with the same assumptions used by SAIC, and concluded the failure probability to be 1.9 x 10^{-6}. Their report is included as Appendix F of this report.

The NESC independent assessment considered that the wire-to-wire "smart" short probability had a high uncertainty because of the need for refined data mining including unknown aging factors and the level of induced maintenance damage. The Darlington failure probability assumptions were considered neither conservative nor optimistic; aging effects were not incorporated. A known limitation of Darlington failure prediction was based on the PRISM® and MIL-HDBK-217 approach (MIL-HDBK-217 is meant to be a design trade tool, not an absolute source for field or in-service failure predictions).

A dynamic system level approach was used for the NESC PRA, refining the Ames' PRA. It incorporated model elements for evolution of wire damage (including aging) over OV-103's lifetime, the causes of initial damage, the effects of routine and major maintenance, and post 1999 improvements. Unlike the Ames' PRA, only failures occurring during docked operations are considered. This dynamic model takes appropriate credit for the proposed use of BITE check on-orbit and the 5-hour RJD powered-on docked window for Darlington failure.

7.5.1 RJD Wire-To-Wire "Smart" Short Failure Mode

1. Using the Program's 4 x 3 Risk Matrix (shown in Figure 6.2-1), the wire-to-wire "smart" short PRA likelihood computed by the NESC is infrequent (~4 x 10^{-3} for 28 flights or 1.5 x 10^{-4} per flight). The consequence is catastrophic. See Figure 7.5.1-1. *Note that this numeric result is essentially the same as the least favorable result that the Program had initially considered.*
2. NESC's wire PRA number has high uncertainty because the effects of wire aging and the level of maintenance-induced wire damage presently are unknown.
3. Additional contributors to the NESC PRA uncertainty were the possibility of latent undetected damage, consideration that maintenance-induced damage may have a high likelihood of physical co-alignment amongst conductors, and the possibility of arc tracking effects spreading current within a bundle.
4. High variability in the various RJD wire PRAs calls into question using these calculated probabilities as justification for flight rationale.
5. A large exposure window of vulnerability to an inadvertent firing from this failure mode exists for the flight crew (175 hours/mission) and ground personnel (70% of turnaround processing).
6. Given PRA uncertainties, unknown susceptibility of RJD wire to arc tracking, and the large exposure window, options to mitigate risk are performing 100% wire inspection or wire modification. NESC recommended implementing a RJD wire modification before STS-115/12A.



Assumptions:

- 175-hour docked exposure risk per flight
- 1700-hours powered-on exposure risk per vehicle turnaround (except Ames who used frequency of wire damage occurrence)
- 4,000 feet of the 150 miles of Orbiter wiring is RJD valve coil wire
- No aging effects
- Only identified (i.e. known) failure modes

NESC using dynamic wire model, Ames and other data (V. Volovoi, 8/19/04, 4.0E-3)

Ames using PRACA data and assumptions (K. Datta, 10/29/03, 3.9E-3)

SAIC et. al. for PRCB using statistical methods w/ ground maintenance experience (5/26/04, 2.5E-4)

SAIC using Bayesian methods and FAA data (1/9/04, 3.9E-5)

Figure 7.5.1-1. Wire-to-Wire "Smart" Short Aggregated Failure Probability for 28 Flights

7.5.2 Darlington Pair Failure Mode

1. Using the Program's 4 x 3 Risk Matrix, the Darlington PRA likelihood is infrequent (~3 x 10^{-4} for 28 flights or 1.18 X 10^{-5} per flight). The consequence is catastrophic. *Note that this numeric result is approximately three orders of magnitude less favorable than the Program's estimate, and is very close to the Honeywell (RJD original equipment manufacturer) analysis (see Figure 7.5.2-1).*

2. The key difference between the NESC analysis and the SAIC analysis is the distribution of "shorted" failures as a percentage of failed devices. The basic part Failure In Time (FIT) rates derived from different sources (AT&T Reliability Handbook and PRISM®) are comparable.

3. There are known limitations with both the SSP and NESC Darlington PRAs (i.e., no aging was assumed and the use of PRISM® and MIL-HDBK-217 for in-service failure predictions *is not recommended*). Darlington failure by analyses has estimates that vary by approximately three orders of magnitude over the life of the program as shown in Figure 7.5.2-2.

4. DPA of Darlingtons can provide critical aging and manufacturing defect information which cannot be captured in a PRA estimate.

5. The Master Verification Plan requires test of Criticality 1/1 (i.e., catastrophic/zero-fault-tolerant) functions before every flight. The RJD is currently addressed via BITE with a binary (0 or 1) result. Adding a leakage current test of all Darlingtons before each flight would be a far superior health check, identifying outliers and establishing a baseline for each device that can then be trended over the life of the Orbiter.

6. Because of PRA uncertainties and limitations, zero-fault-tolerance of the RJD circuit design, and the potential for undiscovered latent defects or unknown failure modes, the majority of the technical team and slightly more than one half of the NRB recommended redesign of the RJD box to be at least single-fault-tolerant against the dual fault tolerant requirement. This can be accomplished by incorporating high-side and low-side switching. The scope of such a change may possibly be limited to a redesign of the RJD heat sink assemblies and BITE circuit with the use of HEXFET switches, in lieu of bipolar power transistors, as the drive signals are transformer coupled. Such a change would improve the fault tolerance of the RJD box driver switches by approximately a factor of 10^6 and make the design more consistent with normal practice for circuits of such criticality, the penalty being reduction of reliability for normal firing by a factor of two. Note that the electronics are considered to be much more reliable than the valves, and that the probability of a failure to energize a thruster will be dominated by mechanical failure modes of the valve.

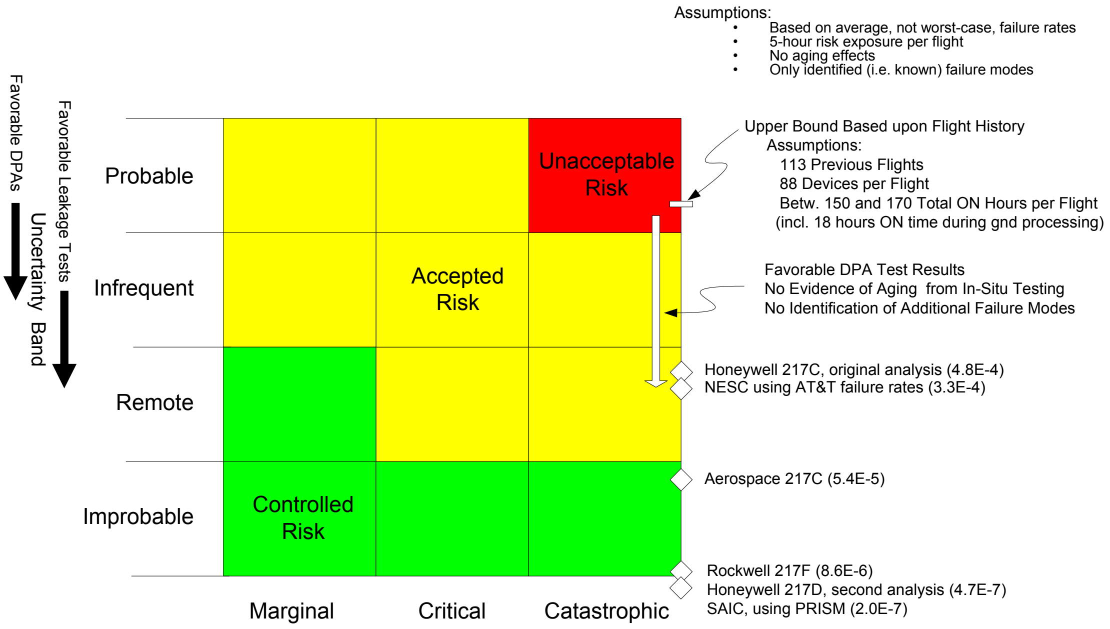


Figure 7.5.2-1. Darlington Transistor Aggregated Failure Probability for 28 Flights

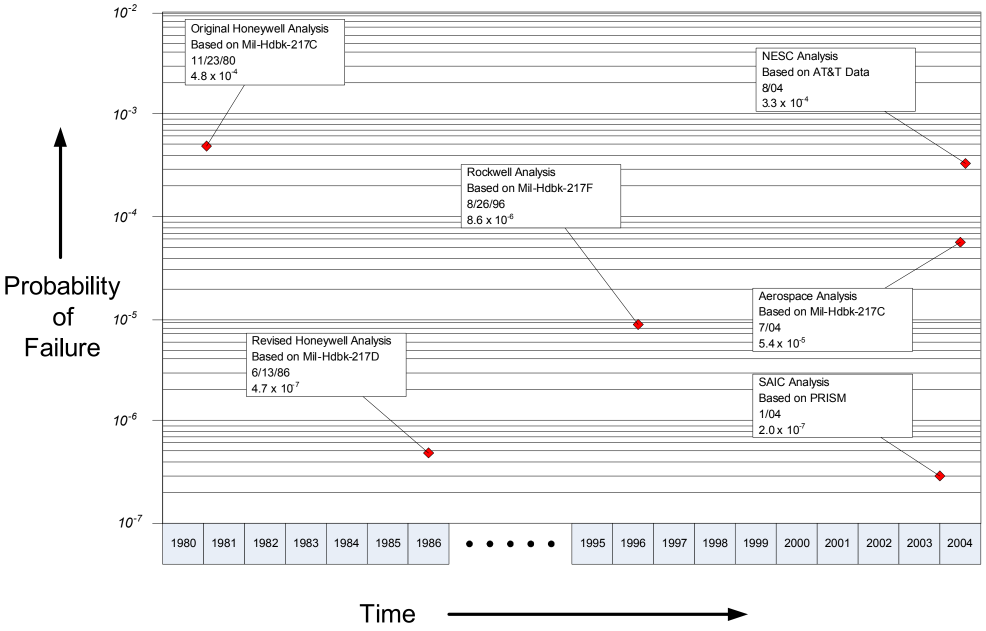


Figure 7.5.2-2. Darlington Transistor Failure Analysis History

7.5.3 Recommendations on Improving NESC PRA Estimates for Wire-to-Wire "Smart" Short Failure Mode

The probability of wire-to-wire "smart" shorts directly depends on the number of damaged wires in an Orbiter at any given point in time. A model for the evolution of this damage has been created, but the output of the model is dramatically affected by several input parameters. These input parameters can be estimated with satisfying precision if the PRACA database allows retrieval of the following information:

1. A separate count for each Orbiter shuttle of the instances of relevant significant damage (damaged and exposed conductors) for each occurrence of both routine and major maintenance.
2. An indication of whether a repaired/replaced wire was from the original installation or whether there was a prior history for this wire segment (if a prior history exists, it should be readily available).

3. An indication whether neighboring wires are damaged as well (and whether there was an apparent common cause or not).
4. Classification of these instances should be assigned with respect to the likely cause of this damage. While a detailed categorization is very desirable, at the minimum, the following categories should be provided:
    a. Initial defects: Defects that existed since the original installation. This category should not include installation errors that have led to subsequent wire damage;
    b. Improper installation: The wire damage is traceable to installation errors that created abnormally adverse conditions for the wiring;
    c. Maintenance-induced damage; and
    d. All other causes (vibration, aging, etc.).
5. Indication of whether the wire is easily accessible for inspection and for other maintenance traffic.

In addition to PRACA's reporting of aspects of the wire damage, quantifying the reliability of visual wire inspection processes (probability of detection) would better estimate the total number of significant damage instances.

New methods may be able to better detect damage, and this could dramatically alter the PRA estimates. Serious consideration should be given to the feasibility of installing sensors (chemical or acoustic sensors) capable of detecting the occurrence of wire shorts (including intermittent ones). This would greatly improve confidence in the observed frequency of shorts. Also, continue to search for a credible test method to assess wire age degradation for input into wire evolution model.

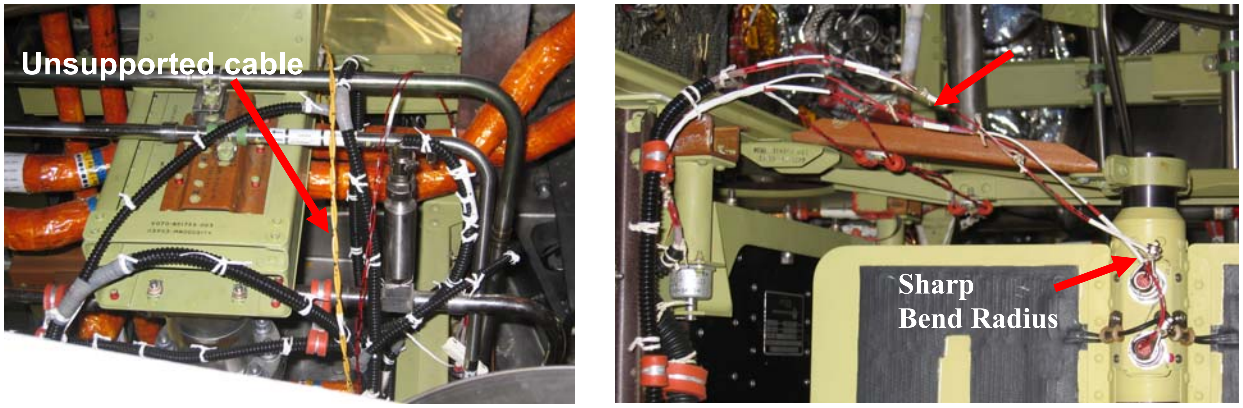
8.0 FINDINGS, OBSERVATIONS and RECOMMENDATIONS

8.1 Findings from KSC Site Inspection

The following concerns arose during KSC's site visit of the OV-105, Hypergolic Maintenance Facility, and NASA Shuttle Logistics Depot (NSLD):

F-1. A number of small diameter Orbiter cables with unsupported lengths of 12-16 inches were found (Figure 8.1-1). Boeing Desk Instruction specifies distance from connector to first clamp is 6" to 12" and the distance from clamp to clamp is as follows:

Harness Diameter	Clamp Distance
1/8" to 7/16"	6" to 8"
1/2" to 11/16"	8" to 12"
3/4" to 1-1/2"	15" max
Greater than 1-1/2"	Special evaluation



Aft bay

Fwd Reaction Control System (RCS)
Pod Heater

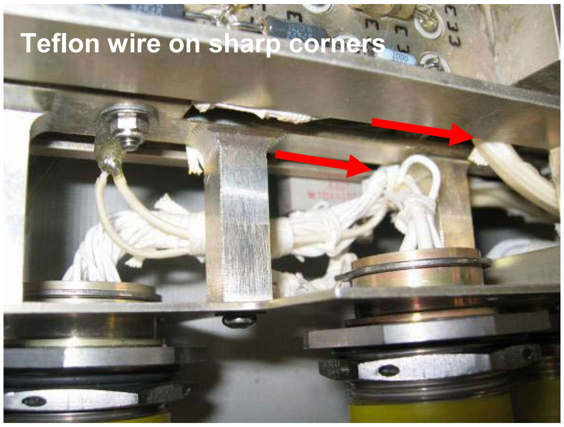
Figure 8.1-1. Orbiter Cables with Unsupported Lengths

F-2. Several cases where wire was bent to tighter bend radius than specification allows.

<u>Note</u>: **Boeing spec ML0303-0014, page 16, paragraph 3.5.6, [8] allows 10 times the diameter of the largest overall wire or cable within the bundle with an exception, if the 10 times cannot be met, 4 times is allowed provided the cable is supported within 4 inches of the termination.**

F-3. Unprotected wire bundles resting on bracket edges in upper equipment wiring area violates NSTS 8080-1 Std. 142, p. 3-285.

F-4. Teflon-insulated wires contacting sharp corners within the RJD box violates the NSTS 8080-1 Std., 142, p. 3-285 (Figure 8.1-2).



RJD Box Connector Area

Figure 8.1-2. Teflon-insulated wires contacting sharp corners within the RJD box

F-5. Temporary Lexan wire protection covers charged enough to raise hairs - electrostatic discharge (ESD) concern (reference ESD requirement NSTS 07700 Volume X - Book 1 (change number 303 dated 6-23-04), pages 3-261 through 3-262A).

F-6. Darlington health requires integrity of the redundant back electromotive force (EMF) suppression network residing at each thruster valve. Proper functionality of EMF suppression is verified every 4-7 flights during WSTF depot thruster testing, but not verified flight to flight. Master Verification Plan (NSTS 07700-10-MVP-01, rev. D, paragraph 3.7.3, p. 7) requires all Crit 1/1 functions to be verified before every flight unless the test is considered to be invasive or illogical.

8.2 Observations

O-1. No occurrence of an inadvertent thruster firing has been observed in flight history and the present process of flight data review has not surfaced signs of impending failure/fault (although chance for a telemetry "escape" exists).

O-2. The current RJD circuit violates fail ops/fail safe (two fault tolerant) requirement for Crit 1 avionics function in 38 driver circuits.

O-3. Wire short failures from latent causes typically occur suddenly without prior warning. STS-93 wire short may have flown without incident for 11 flights (5 years) based on post-flight analysis of oxidation layer on conductor.

O-4. NESC analysis of Federal Aviation Administration (FAA) data shows that aircraft wiring flaws/failures have an aging component not considered in the existing predictions/risk calculations.

O-5. The Program has had conductive particle and corrosion problems in EEE parts similar to the Darlingtons that have caused in flight anomalies (i.e., STS-58). Many industry GIDEP alerts for transistors similar to RJD Darlingtons involve failure of PIND tests to screen for conductive contaminants.

O-6. During a spot audit of the RJD connector layouts, the 50P9967 connector pinning had an RJD command pin next to an Orbital Maneuvering Engine command pin. For an illustration, refer to Volume II, Appendix B of this report.

O-7. A typical RJD box-to-valve solenoid wiring harness is a combination of 20 American Wire Gage (AWG) single conductors, twisted-shielded pairs, and unshielded twisted quads. While shielded twisted pairs are more immune to induced damage and electrical noise, twisted pairs/quads are more prone to shorting and sustaining an arc track event.

O-8. The RJD box-to-valve solenoid harnesses also include 28 VDC heater circuit wiring. Twisting and shielding of heater circuit wiring enhances arc track susceptibility and propagation to adjacent valve solenoid coil wires.

O-9. There currently is no definitive chemical, mechanical, or electrical testing that can determine if polyimide wire insulation has degraded or "aged".

O-10. Using identical assumptions, the proposed high-side/low-side switching (single-fault-tolerant) design would be ~10^6 times less susceptible to inadvertent firing than the current zero-fault-tolerant design. As a result, the single-fault-tolerant design would be 2 times less likely to fire when needed.

O-11. All PRA predictions are based on per-flight risk. Using the small number approximation, risk will accumulate linearly with the number of flights (i.e., N times more likely to occur at least once during N flight regime).

O-12. Insufficient information was provided on Darlington pair screening details. HR ORBI 055 cites OPPL requirements, but NESC-requested specifics for screening tests have not been provided.

O-13. PRACA and Corrective Action Record (CAR) searches found 58 separate RJD documents (with 8 pre-STS-01 events) including blown fuses traced to ground support equipment (GSE), failed leakage/trickle current tests, and other OMS simulator or ground handling-induced problems. Note that the Darlington transistors were replaced when fuses were found blown.

Conclusions from the PRACA search were that there were no RJD "stuck-ON" failures when connected to live thrusters; other RJD components could have been degraded by external stresses experienced during these ground events; the RJD is susceptible to damage by external events; and mapping of these 58 events by RJD S/N excluded the currently-installed RJDs and 4 of 6 flight spare RJDs from this concern.

O-14. HR ORBI 055 (rev. E) and Failure Mode and Effects/CIL (FMEA/CIL) 05-1-F-FC6242 & 05-1-FC6342 do not adequately address the effects of RJD part aging. Reports state that RJDs are certified for 10,000 hours or 100 missions, equivalent to 10 years, but the actual physical age of some parts is much greater (e.g., 25 years).

O-15. Six (6) GIDEP alerts exist on Darlington pair transistor types of similar age and make. (Note: Screening to exclude all Shuttle parts from Alerts is in progress).

O-16. During the KSC site visit, un-jacketed loose braid at the connector back shells (tag-ring) was observed in the Orbiter cabling.

O-17. During the KSC site visit, un-encapsulated stainless steel braided hoses were observed in the wire harness area.

8.3 Recommendations

Note: The NESC did not review the manifold auto-close software modification as effective for the next two flights. All references to actions required before STS-115/12A assume the Program will ensure that the software modification is in place and verified effective before STS-114.

R-1. Review the build records to compare GIDEP alerts in the NESC report to Orbiter Darlington pairs. Refer to Section 7.4.2.4.

R-2. As soon as possible, but NLT STS-115/12A, conduct Darlington tests proposed by NESC. Refer to Section 7.4.2.2, Section 7.4.2.3, and to Appendix D, Darlington Transistor Test Plan.

R-3. As soon as possible, but NLT STS-115/12A, institute on-orbit crew procedure changes (minimize RJD powered on time while docked and check RJD BITE circuitry before RJD power on).

R-4. As soon as possible, but NLT STS-115/12A, update program Darlington PRA considering NESC results and stated limitations. PRA should not only address all credible failure modes identified by NESC, but also capture the accumulated risks over the life of the remaining flights.

R-5. As soon as possible, but NLT STS-115/12A, modify the Operations and Maintenance Requirements and Specifications Document (OMRSD) to perform a Darlington transistor leakage current test for every vehicle turnaround. If feasible, reassign RJD channel monitor outputs at MDM from bi-level to analog channels to obtain greater leakage current data in-situ. Consider using RJD channel leakage current data from NSLD operations to look for prior degradation trends.

R-6. As soon as possible, but NLT STS-115/12A, verify all harness connectors from RJDs to valve solenoids adhere to the requirement to separate power and critical signal pins (reference NSTS 8080-1 Std. 32, p. 3-65).

R-7. As soon as possible, but NLT STS-115/12A, replace the 76 RJD valve coil wires with more resilient and better-protected wiring. This could be Teflon tape or convolute tube over existing wires, or replacement with most resilient configuration from proposed NESC wire tests.

R-8. Update the Program's wire PRA considering NESC results and stated limitations as a way to introduce wire aging effects. Refer to Section 7.3.1 and to Appendix G, Wiring Damage Analyses for STS OV-103.

R-9. Conduct wire tests proposed by NESC. Refer to Appendix E, RJD Shielded Wire Dry Arc-Track Test.

R-10. Investigate ways to eliminate FOD concern with shield braid termination wires in connector backshell area (e.g., wrap with Teflon tape or add conformal coating, "baggie" connector body and exit wire during ground operations).

R-11. Investigate use of inert gas wire dielectric testing for detecting insulation defects during OMM wiring inspection.

R-12. Ensure effort is underway to update HR ORBI-055 and that it addresses additional failure modes in the NESC report.

R-13. Review OMM ESD control procedures for violations of ESD protection outlined in NSTS 07700 Volume X - Book 1 (change number 303 dated 6-23-04), pages 3-261 through 3-262A. Investigate use of ESD "sniffers" at Orbiter Processing Facility (OPF).

R-14. Review in-flight telemetry data to identify momentary primary RCS inadvertent firings that may have either escaped observation or were mischaracterized as invalid due to weak signal-to-noise. Refer to Section 7.2.2.

R-15. Program should review its use of MIL-HDBK-217 in PRAs considering the known limitations of this method as a field (in-service) failure prediction tool.

9.0 REFERENCES

[1] Koushik Datta. Ames Research Center, "Risk Assessment of Wire Failures Causing Uncommanded Orbiter RCS Firing While Docked at the ISS", October 29, 2003

[2] Samandar Roshan-Zamir (SAIC). "Point Estimate Analysis of the Probability of Wire-to-Wire Short in the RCS Area", January 9, 2004; updated May 26, 2004

[3] PRISM®, *RAC-STD-6500, PRISM System Reliability Assessment Software Tool*, Reliability Analysis Center, Rome, New York.

[4] *MIL-HDBK-217, Reliability Prediction of Electronic Equipment*, Revisions A through F/Notice 2 (28 February 1995), Department of Defense, Washington DC, 1997.

[5] *RAC-STD-6300, FMD-97, Failure Mode/Mechanism Distributions*, Reliability Analysis Center, Rome, New York. Note: Previous editions of this document were available; e.g., FMD-91 dated 1991.

[6] Volovoi, V., Georgia Tech Research Engineer, "Probabilistic Risk Assessment of Failures Leading to the Inadvertent Firing of Thrusters while Orbiter is Docked to the International Space Station**,** Version 10.0**".**

[7] Thomas W., "Crow-AMSAA Analysis of Orbiter Wiring Shorts", NASA GSFC presentation report to NESC Space Shuttle Orbiter RJD ITA/I, May 21, 2004, 3 pp. [Based on data abstracted from Appendix D, "Known Short Circuit Incidents…" of "Orbiter Interconnect Short Circuits", P. Krause, Boeing OV Engineering, May 10, 2004, 15 pp.].

[8] Boeing Spec ML0303-0014, page 16, paragraph 3.5.6.

[9] NASA Orbiter Sampling Test Results and Analysis (WIDAS report, N224-RPT16SE0)
PBMA: "Aging Wire Study by NASA" Boeing_Orbiter.pdf, September 16, 2000.

[10] Boeing "New Wire Insulation Study for Potential Orbiter Use"
PBMA: Boeing Shuttle Wire Study; New_Wire_Insulation_Study.pdf, June 5, 2000.

10.0 LIST OF ACRONYMS

Acronym	Definition
A	amps
ARC	Ames Research Center
AWG	American Wire Gage
BITE	Built In Test Equipment
BN	Bayesian Network (or BBN for Bayesian (belief) networks)
CA	Crow-Army Material Systems Analysis Activity
CAR	Corrective Action Record
CDF	Cumulative Density of Failure
CFR	Constant Failure Rate
CIL	Critical Items List
DPA	Destructive Physical Analysis
EDS	Energy Dissipation Spectroscopy
EMF	Electromotive Force
ESD	Electrostatic Discharge
EVA	Extravehicular Activity
FAA	Federal Aviation Administration
FAR	Federal Air Regulation
FIT	Failure In Time
FMD	Failure Mode/Distribution Database
FMEA	Failure Mode & Effects Analysis
FMECA	Failure Mode, Effect, and Criticality Analysis
FOD	Function Operational Design
FT	Fault Tree
FTA	Fault Tree Analysis
GIDEP	Government/Industry Data Exchange Program
GPC	General Purpose Computer
GRC	Glenn Research Center
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
HPP	Homogeneous Poisson Process
HR	Hazard Report
ISS	International Space Station
ITA/I	Independent Technical Assessment/Inspection
JSC	Johnson Space Center
KSC	Kennedy Space Center
kW	Kilowatt
LaRC	Langley Research Center
LCC	Launch Control Center
LRU	Line Replaceable Unit or Logistical Replaceable Unit
MDM	Multiplexer/Demultiplexer
MECO	Main Engine Cutoff

Acronym	Definition
MOSFET	Metal Oxide Semiconductor Field Effect Transistor
MVP	Master Verification Plan
NASA	National Aeronautics and Space Administration
NESC	NASA Engineering and Safety Center
NIA	National Institute of Aerospace
NLT	No Later Than
NRB	NESC Review Board
NSLD	NASA Shuttle Logistics Depot
NSTS	National Space Transportation System
OMM	Orbiter Major Maintenance
OMRSD	Operations and Maintenance Requirements and Specifications Document
OMS	Orbital Maneuvering System
OPF	Orbiter Processing Facility
OPPL	Orbiter Project Parts List
OSC	Orbital Sciences Corporation
OV	Orbiter Vehicle
OWWG	Orbiter Wire Working Group
Pf	Probability of Failure
PIND	Particle Induced Noise Detection
PRA	Probabilistic Risk Assessment or Analysis
PRACA	Problem Reporting and Correction Action
PRCB	Program Requirements Control Board
RAC	Reliability Analysis Center
RCS	Reaction Control System
RGA	Residual Gas Analysis
RJD	Reaction Jet Driver
S&MA	Safety & Mission Assurance
SAIC	Science Applications International Corporation
SCAN	Shuttle Connector Analysis Network
SD	Significant Damage
STS	Space Transportation System
USA	United Space Alliance
V	Volts
VDC	Volts Direct Current
W	Watt
WIDAS	Wire Insulation Degradation Analysis System
WPAFB	Wright Patterson Air Force Base
WSTF	White Sands Test Facility

11.0 MINORITY REPORT (dissenting opinions)

At the NESC Review Board held on August 17, 2004, intense discussions resulted in split positions for the recommended course of action to be forwarded by the NESC. Five of the seven assessment team members recommended that the RJD high-side/low-side switch redesign commence immediately. Slightly more than one half of the NESC Review Board agreed with this approach while the remainder wanted to pursue additional data through test and evaluation before delivering a recommendation on the RJD redesign. The NESC Director's decision was to go forward with the later recommendation.

12.0 LESSONS LEARNED

This issue surfaced after a review of all integrated hazards by the ISS was directed after the *Columbia* accident, and ISS withheld signature on the Non-Conformance Report forcing the system to respond. The SSP Hazard Report with waiver rationale was last updated in 1999 and did not account for all failure modes.

Whereas some of the transistors and wires in the Orbiter fleet are 25+ years old, no data exists on aging effects and no test is currently available to assess age degradation of the Shuttle's Kapton® wiring. The various PRAs performed by both the Shuttle Program and the NESC produced a wide range of results. All transistor PRAs used MIL-HDBK-217 as an absolute source for field (in-service) failure prediction, despite the handbook's known limitation as a design trade tool.

Because of uncertainty in the various PRAs, the NESC recommended electrical characterization testing and a DPA of the RJD transistors from flight assets to determine the potential effects of aging and manufacturing defects. The NESC also recommended adding a new preflight leakage current test to assess the health of the transistors and the replacement of RJD valve coil wires with new, better protected wiring that would be separated from power wires.

Lesson: Programs that share physical interfaces, and therefore risks, should ensure that responsibilities for integrated hazards are clearly defined and that the system requires periodic reviews of these hazard reports.

Lesson: The effects of aging, operation, and environmental exposure should be factored into the expected operational life of new vehicle designs. Reliability prediction methods should include aging effects.

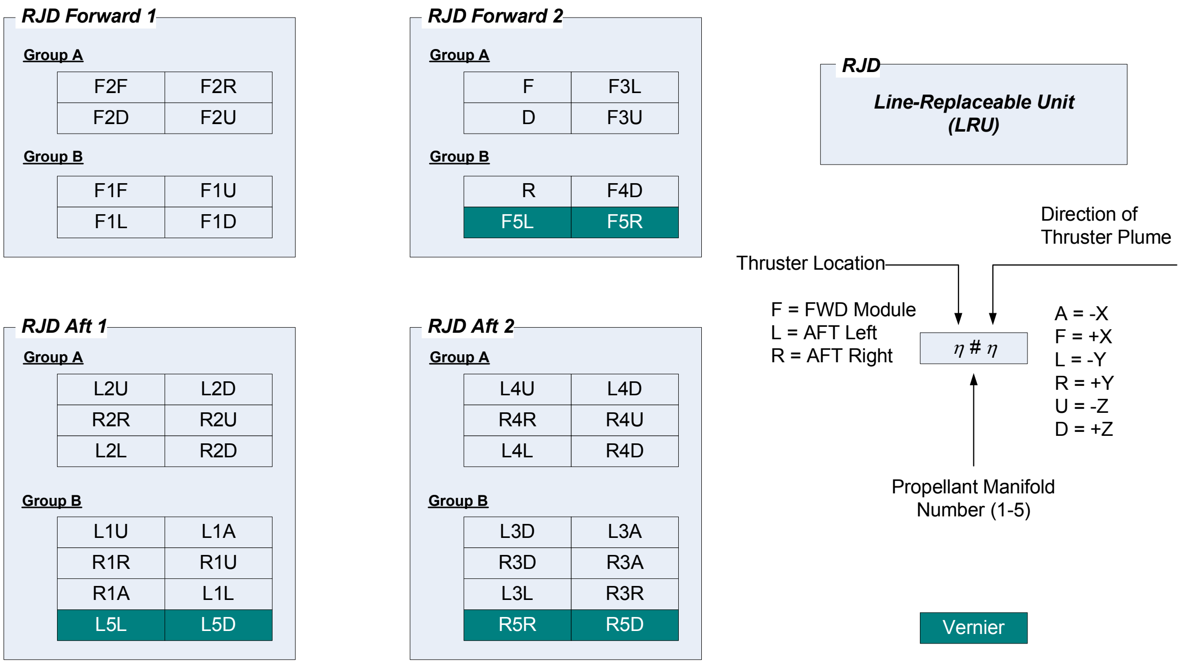
Lesson: MIL-HDBK-217 is not suited as an absolute quantitative tool to predict the likelihood of electronic part failures in space systems and does not consider parts aging or stresses accumulated during field use, leading to potential over-estimation of part reliability.

VOLUME II: APPENDICES

A. RJD Illustrations
B. Consolidated Failure Mode Listing
C. PRA of Failures Leading to the Inadvertent Firing of Thrusters While the Orbiter is Docked to the International Space Station
D. Darlington Transistor Test Plan
E. Orbiter Wire Test Plan
F. Aerospace Darlington Transistor Assessment Report
G. Wiring Damage Analyses for STS OV-103
H. Team Member Biographies

Appendix A

RJD Illustrations



RJD Forward 1

Group A

F2F	F2R
F2D	F2U

Group B

F1F	F1U
F1L	F1D

RJD Forward 2

Group A

F	F3L
D	F3U

Group B

R	F4D
F5L	F5R

RJD Aft 1

Group A

L2U	L2D
R2R	R2U
L2L	R2D

Group B

L1U	L1A
R1R	R1U
R1A	L1L
L5L	L5D

RJD Aft 2

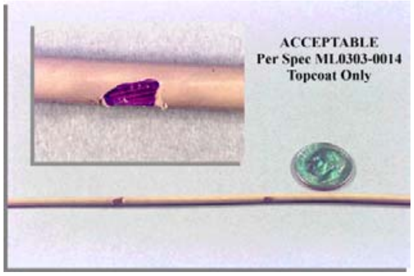
Group A

L4U	L4D
R4R	R4U
L4L	R4D

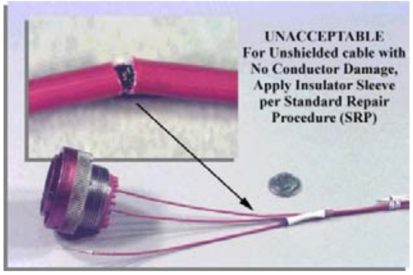
Group B

L3D	L3A
R3D	R3A
L3L	R3R
R5R	R5D

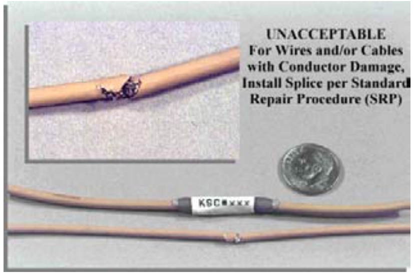
RJD Thruster Assignments



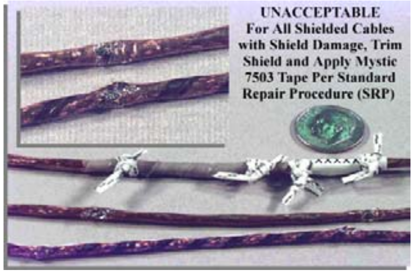
ACCEPTABLE
Per Spec ML0303-0014
Topcoat Only



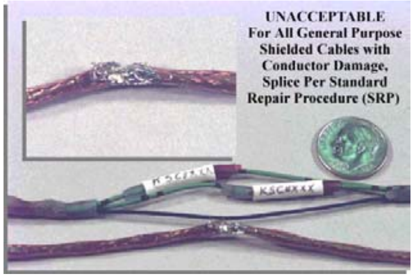
UNACCEPTABLE
For Unshielded cable with
No Conductor Damage,
Apply Insulator Sleeve
per Standard Repair
Procedure (SRP)



UNACCEPTABLE
For Wires and/or Cables
with Conductor Damage,
Install Splice per Standard
Repair Procedure (SRP)



UNACCEPTABLE
For All Shielded Cables
with Shield Damage, Trim
Shield and Apply Mystic
7503 Tape Per Standard
Repair Procedure (SRP)



UNACCEPTABLE
For All General Purpose
Shielded Cables with
Conductor Damage,
Splice Per Standard
Repair Procedure (SRP)

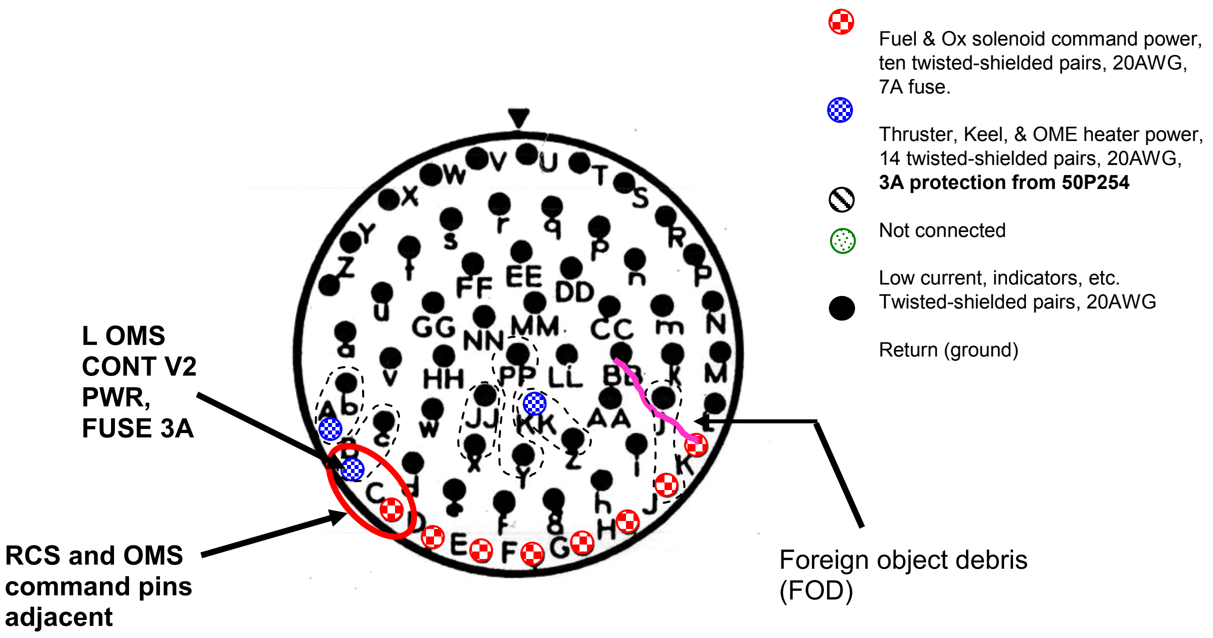
Source: Orbiter Wiring Discrepancy & Repair, Course Presentation, 4/21/00, Boeing

Consideration of Possible RJD Options

Approach	Options	PROs	CONs
No Hardware Changes	• Limit RJD on time • Check BITE prior to each power on • Review 1.5 second requirement - Susceptibility - Response time	• Retains RJD box and wiring configuration that has not shown prior problems in flight	• Requires waivers • Susceptible to identified failure modes • Remote but credible risks remain
Wire Only Change	• Shielded wire for RJD outputs	• Provides increased protection for wire-to-wire "smart" shorts • Lowers risk to KSC ground ops personnel	• Increases susceptibility for wire-to-ground shorts • Does not address Darlington shorts and may increase their likelihood
Wire & RJD Box Changes	• Wire & RJD Dual High Switches	• Simple fix for identified most likely failure modes • Does not require return wiring changes	• Slightly more complex • Slightly lower reliability for normal firing
	• Wire & RJD High & Low Switches	• Robust circuit change that addresses identified failure modes plus others such as transistor short without fuse opening	• Slightly more complex • Slightly lower reliability for normal firing • Requires return wiring changes

From Observation O-6.

Connector Pinout - RJDA1-to-Thruster Harness (+Y Thruster)
Functions: Fuel & Ox solenoid command power, heater power
Location: Aft Body/Doghouse
Reference Designator: **50P9967** Type: 24-61 plug, (61) 20ga. Contacts
Observations: Most thruster coil pins are separated from 28 VDC pins. Bent pins can only short or disable thruster **except for noted pins below**


Fuel & Ox solenoid command power, ten twisted-shielded pairs, 20AWG, 7A fuse.
Thruster, Keel, & OME heater power, 14 twisted-shielded pairs, 20AWG, **3A protection from 50P254**
Not connected
Low current, indicators, etc. Twisted-shielded pairs, 20AWG
Return (ground)
L OMS CONT V2 PWR, FUSE 3A
RCS and OMS command pins adjacent
Foreign object debris (FOD)
W
V
U
T
S
R
P
N
M
L
K
J
H
G
F
E
D
C
B
A
X
Y
Z
a
b
c
d
e
f
g
h
i
j
k
m
n
p
q
r
s
t
u
v
w
x
y
z
AA
BB
CC
DD
EE
FF
GG
HH
JJ
KK
LL
MM
NN
PP

Appendix B

Consolidated Failure Mode Listing

8/8/2004	**Failure Modes Resulting in an Orbiter Reaction Control Jet Inadvertent Firing**	Rick Gilbrech
	NESC Independent Technical Assessment	757-864-2400
	Color coded mapping to FTA (Vitali)	
	not modeled	🟥
	directly modeled	🟩
	inferred	🟨
Mode #	Description	Probability
🟥 1	Erroneous output from multiplexer/demultiplexer (requires multiple simultaneous synchronous signals).	Improbable
🟥 2	Erroneous output from General Purpose Computer.	Improbable
🟥 3	Pin-to-pin short (hot) – RJD output command pin to command pin short resulting in two thrusters firing instead of selected thruster or RJD output command pin to power resulting in inadvertent thruster firing.	Remote
🟩 4	Valve coil command wire short to 28VDC conductor due to undetected mechanical damage to bundle during maintenance or inspection (e.g. removal or work platform crushes bundle but can't be seen since platform required for inspection).	Remote
🟩 5	Valve coil command wire short to 28VDC conductor due to undetected manufacturing flaw in bundle.	Remote
🟩 6	Valve coil command wire short to 28VDC conductor due to in-flight mechanical damage to bundle.	Remote
🟩 7	Valve coil command wire short to 28VDC conductor due to solvent attack of wire bundle insulation. Solvents, Skydrol, NH4, all take weeks to months of exposure at elevated temps (>100-200C) to drop tensile a few %. Only ammonium hydroxide (2d at RT) and sodium hydroxide 10% (5d at RT) are catastrophic. Water for 28d at 135C loses 50% tensile.	Improbable

8/8/2004	**Failure Modes Resulting in an Orbiter Reaction Control Jet Inadvertent Firing**	Rick Gilbrech
	NESC Independent Technical Assessment	757-864-2400
	Color coded mapping to FTA (Vitali)	
	not modeled	🟥
	directly modeled	🟩
	inferred	🟨
Mode #	Description	Probability
🟩 8	Valve coil command wire short to 28VDC conductor due to conductive liquid between conductors and cracked insulation.	Improbable
🟨 9	Valve coil command wire short to 28VDC conductor due to metallic chip wedged in bundle.	Remote
🟥 10	Valve coil command wire short to 28VDC conductor due to shield braid wire foreign object debris (~36AWG strand) bridging between 28VDC and command line through ring-cracks in insulation. Note: Braid foreign object debris would need to "float" over from nearby LRU that uses tag-ring back shell with shielded wire.	Improbable
🟩 11	Arc tracking in wire bundle 28VDC wire short to ground where bundle contains valve coil command wire and arc propagates current to the coil wire. A typical RJD-to-thruster bundle (22P67 or 50P9967) has (4 to 14) 28VDC wires shielded and unshielded, (12 to 16) return wires, and (8 to 10) command wires shielded and unshielded.	Remote
🟨 12	Low resistance shorts between RJD control wiring and any voltage sources capable of 12.5V or more and 1A or more, need to consider over voltage conditions and application of high voltage to electrical ground.	Remote
🟩 13	Wire insulation flaws due to aging cause valve coil command wire to contact 28VDC conductor in a bundle.	Remote
🟩 14	Motion of unsupported bundle span causes chafing and short of valve coil command wire to 28 volt conductor.	Remote

8/8/2004	**Failure Modes Resulting in an Orbiter Reaction Control Jet Inadvertent Firing**	Rick Gilbrech
	NESC Independent Technical Assessment	757-864-2400
	Color coded mapping to FTA (Vitali)	
	not modeled	🟥
	directly modeled	🟩
	inferred	🟨
Mode #	Description	Probability
🟩 15	Internal RJD box wire short of any driver or output Darlington transistor emitter or base lead wire to 28VDC conductor or terminal. Photos taken at KSC do show wires resting on metal chassis edges in connector area. However, wire appears to be Teflon-coated. Cold flow of insulation would most likely have occurred much earlier. Low probability of failure (abrasion of wire insulation with chassis edges may be possible).	Improbable
🟩 16	Excessive leakage current due to aging, degraded metallization, or leaky hermetic seal in a driver Darlington transistor.	Remote
🟨 17	RJD box internal wire short of any Darlington transistor emitter or base lead wire to 28 volt conductor or terminal.	Improbable
🟩 18	Shorted Darlington output transistor caused by turn on into an intermittent valve coil command wire short to chassis that shorts transistor but does not open 7A fuse (requires two simo conditions – thruster firing during intermittent short).	Remote
🟨 19	Collector to emitter short of Q2 of any output Darlington transistor of a resistance of less than 6Ω. This short will result in greater than 1 of current available for both the oxidizer and fuel valves.	Remote
🟨 20	Collector to base short of Q1 of any output Darlington transistor. A short being defined as any resistance of less that 6kΩ. This short will result in greater than 1A of current available for both the oxidizer and fuel valves.	Remote
🟨 21	Collector to base short of Q2 of any output Darlington transistor. A short being defined as any resistance of less that 500Ω. This short will result in greater than 1 Amp of current available for both the oxidizer and fuel valves. (This is the same case as a collector to emitter short of Q1).	Remote

8/8/2004	**Failure Modes Resulting in an Orbiter Reaction Control Jet Inadvertent Firing**	Rick Gilbrech
	NESC Independent Technical Assessment	757-864-2400
	Color coded mapping to FTA (Vitali)	
	not modeled	🟥
	directly modeled	🟩
	inferred	🟨
Mode #	Description	Probability
🟨 22	Arc tracking in wire bundle 28VDC wire short to return wire where bundle contains valve coil command wire and arc propagates current to the coil wire. A typical RJD-to-thruster bundle (22P67) has (4) 28VDC wires, (12) return wires, and (8) command wires.	Remote
🟨 23	Internal conductive contaminant in any Darlington transistor.	Remote
🟨 24	External conductive contaminant between Darlington transistor case (at collector potential) and the base or emitter pin. This is typically a small dimension and the use of heat sink insulating wafers as is done here can trap a conductive particle in this critical area that over time with vibration and materials properties changes such as slight shrinkage in vacuum can result in a short. Because of the insulating wafer this area will be uncoated. Possible, but not highly likely. Have seen this failure mode occur from time to time.	Improbable
🟨 25	Darlington failure precipitated by ESD event, either during vehicle servicing or an in-flight event. Failure could be immediate (prompt) or can result from prior (latent) damage.	Remote
🟨 26	Ground fault of an unrelated wire or device with sufficient current to damage RJD (return wires or avionics components).	Improbable
🟨 27	Drive transistor base to emitter resistor open circuit. PSPICE modeling on this looked okay, but we will also test at high temperature. Generally, transistor leakage current increases with the resistor open. This would tend to partially turn the Darlington pair on.	Improbable
🟨 28	Ground fault current casing damage to RJD Darlington transistors.	Improbable
🟨 29	Mechanical failure in thruster valve (fuel and ox valve failures required for firing).	Improbable

8/8/2004	**Failure Modes Resulting in an Orbiter Reaction Control Jet Inadvertent Firing**	Rick Gilbrech
	NESC Independent Technical Assessment	757-864-2400
	Color coded mapping to FTA (Vitali)	
	not modeled	🟥
	directly modeled	🟩
	inferred	🟨
Mode #	Description	Probability
🟨 30	Over temperature of RJD box due to heat loop failure. Need to have power to box shut down in the event of over temperature to prevent possibility of uncommanded output. (The RJD box would probably need to get hotter than 125C for this to be an issue, and hopefully limit checking would catch such an event if it were to occur much sooner and shut it down).	Improbable
🟨 31	RJD LRU internal leakage current path that causes the Darlington transistor pair to turn on. The leakage could be caused by:	Not Credible
🟩	Degradation of the isolation transformer in the Darlington driver circuit due to material aging, contamination, or arcing. Not credible. PSPICE analysis has shown insufficient current with transformer short to activate valves.	
🟩	Internal leakage path across circuit board or wiring due to contamination or arc track. Not credible. No circuit board modes due to isolation transformer. Arc track is not likely since there is no evidence of polyimide inside RJD box, and wires are Teflon insulated rather than Kapton.	
🟥 32	Component or subsystem failure inside RJD box that imposes 28VDC or higher voltage on valve coil command wire (i.e., power supply failure, edge connector failure, hook-up wire failure, foreign object debris, logic board failure, or filter circuit failure). Not credible since output line does not go to circuit board but directly to output connector. No power supply interface, no edge connector, logic board, or filter circuit failure identified as credible. Hook-up wire addressed in #15 above.	Not Credible

8/8/2004	**Failure Modes Resulting in an Orbiter Reaction Control Jet Inadvertent Firing**	Rick Gilbrech
	NESC Independent Technical Assessment	757-864-2400
	Color coded mapping to FTA (Vitali)	
	not modeled	🟥
	directly modeled	🟩
	inferred	🟨
Mode #	Description	Probability
🟥 33	Any energy source inadvertently connected to the RJD signal “J2-1 TP1”. This appears to be a test point connected via a 10kW resistor to the base of Q1. This is a critical point sense it provides an energy path into the Darlington pair control signal. This signal terminates at an internal box connector and is not exposed to the environment outside the box. Due to the isolation, this was not considered a credible failure and the probability of failure was assumed to be zero.	Not Credible
🟥 34	Any energy source inadvertently connected to “Jet 1X MDM Out” telemetry signal. This signal is isolated from the valve control signal by 13kW, (12kW in series with a 1.2kW resistor.) A voltage source of +28VDC (or a current source of +1 Amp) connected to this signal will not activate a valve. This mode was not considered a credible failure and the probability of failure was assumed to be zero.	Not Credible
🟥 35	A short across the Control voltage isolation transformer from the input drive power to the output center tap or end tap. Since the transformer is a quadrifilar wound transformer, the input and output transformer wires may be in contact. A short of the transformer input drive power will result in less than 50mA of valve drive current. Since this in insufficient current to actuate the valves, this mode was not considered a credible failure and the probability of failure was assumed to be zero.	Not Credible
🟥 36	The thruster back EMF voltage coupling across the control isolation transformer and stressing the input drive power transistor. Due to the quadrifilar wound transformer there will be substantial capacitance between the input and output wiring. Assuming the worst-case capacitance of 12,000pF, there was insufficient voltage to be a concern to the drive power transistor. This mode was not considered a credible failure and the probability of failure was assumed to be zero.	Not Credible

8/8/2004	**Failure Modes Resulting in an Orbiter Reaction Control Jet Inadvertent Firing**	Rick Gilbrech
	NESC Independent Technical Assessment	757-864-2400
	Color coded mapping to FTA (Vitali)	
	not modeled	🟪
	directly modeled	🟩
	inferred	🟨
Mode #	Description	Probability
🟪 37	Electromagnetic energy coupling into the valve drive wire and inadvertently enabling the Darlington pair. Due to the transformer isolation of the Darlington Pair control voltage; it does not appear that a realistic energy source can couple sufficient energy to activate the valve. This mode was not considered a credible failure and the probability of failure was assumed to be zero.	Not Credible
🟩 38	Cosmic rays deposit charge that can activate and/or short transistors.	Remote
	NOTE: Likelihood based on NSTS 07700-10-MVP-01, rev. D	
	Probable: Will occur several times in the life of the program. A general guideline for likelihood of occurrence would be 1 in 12 to 125 flights ($8.3E^{-2} > X > 8E^{-3}$).	
	Infrequent: Likely to occur sometime in the life of the program. A general guideline for likelihood of occurrence would be 1 in 125 to 1,250 flights ($8E^{-3} > X > 8E^{-4}$).	
	Remote: Unlikely, but possible to occur in the life of the program. A general guideline for likelihood of occurrence would be 1 in 1,250 to 12,500 flights ($8E^{-4} > X > 8E^{-5}$).	
	Improbable: So unlikely that it can be assumed occurrence may not be experienced in the life of the program. A general guideline for likelihood of occurrence would be greater than 1 in 12,500 flights ($X < 8E^{-5}$).	

Appendix C

Probabilistic Risk Assessment of Failures Leading to the Inadvertent Firing of Thrusters while the Orbiter is Docked to the International Space Station

Space Shuttle Reaction Jet Driver Independent Technical Assessment/Inspection (ITA/I)

Report (version 10.0, December 16, 2004)

Prepared by Dr. Vitali V. Volovoi

Georgia Institute of Technology
(404) 894-9810, FAX (404) 894-2760
e-mail: vitali.volovoi@ae.gatech.edu.

Summary

This document describes a quantitative model for assessing risks associated with the inadvertent firing of thrusters while an Orbiter is mated to the International Space Station (ISS). Wire-to-wire “smart” shorts as well as failures of the Darlington pair are considered. Since previous risk assessments of the same problem provided widely varying risk estimates, approaches and assumptions of these assessments are reviewed. Challenges of risk modeling in the context of NASA programs are also discussed. A dynamic model for the amount of wire damage as a function of time was developed to evaluate the probability of a wire-to-wire “smart” short. This model estimates the amount of significant wire damage for a given Orbiter and flight. The relevant significant damage for both wire-to-wire “smart” short and arcing is considered to be exposed and damaged conductors. Initially, the input parameters for this model were obtained using a combination of engineering judgment and a very limited amount of historical data. Consequently, a more detailed analysis of PRACA data has been conducted (see Appendix G) which provides alternative estimates for some of the critical input parameters into the wire damage model. The calculations from both approaches values of significant damage (SD) are used as inputs for fault trees to evaluate the probability of a wire-to-wire “smart” short. While the presence of significant wire damage is necessary for the short to occur, the damage might be dormant for several flights before the failure takes place. The possibility of the delay between the wire damage occurrence and the associated wire short is recognized by introduction of the so-called dynamic basic events. In calculating the probability of Darlington pair failure, the exposure rate is five hours for all 38 thrusters. Model for estimating likelihood of a wire-to-wire “smart” short is based on Orbiter-specific data (OV-103 wire damage data was used to construct the model). The model provides guidelines for collecting and processing relevant historical and experimental data to improve the confidence in predictive power of risk estimates. Strong coupling among the influences of input model parameters on the risk estimates leads to difficulties in conducting traditional sensitivity analysis. Due to the lack of data needed to characterize the input parameters probabilistically, interval-based methods for uncertainty quantification might provide an attractive alternative for the follow-up studies.

Outline

The introduction consists of a general background on reliability and safety predictions for complex, unique systems such as those used by NASA. This is followed by a review of previous risk assessments of inadvertent firing of the Shuttle’s thruster, including the point estimate provided by Samandar Roshan-Zamir (SAIC) [1] and the risk assessment conducted by Koushik Datta (NASA Ames) [2]. The present assessment is focused on the two most credible failure modes: a wire-to-wire “smart” short and failures of a Darlington pair. While a fault tree (Figures C-8 through C-14) is constructed that unites both of these modes, each of the two modes requires a fundamentally distinct approach, and the rest of this document treats them separately. There is a significant amount of information directly or indirectly related to wire-to-wire “smart” shorts and the main challenge is to process this information and assess its relevance. A motivation for the selected approach is provided followed by a construction of a wire damage model that reflects dynamic (time-dependent) characteristics. The output of this model is consequently utilized to calculate probabilities of several critical basic events in the fault tree. Table C-2 lists basic events for wire-to-wire “smart” short. In contrast to Table C-2, there is very little information available on the reliability of Darlington pairs, which makes the analysis relatively simple, but the predictions remain highly uncertain. Table C-3 lists events for the Darlington pair.

Background

As engineering systems became more complex during the second half of twentieth century, the need for comprehensive means to assess and predict their reliability and safety became evident. However, several significant obstacles hampered both the development of new methods and techniques addressing this need and their acceptance by the general engineering community. Probabilistic Risk Assessment (PRA) [3,4] was originally introduced in the context of nuclear plants and after the *Challenger* accident was recognized by NASA as the most appropriate framework for evaluating safety of a system [5]. It has been acknowledged that spacecraft systems and nuclear plants share important characteristics that make the analysis of their safety sufficiently similar: both are complex and highly coupled systems which make them inherently prone to failure [6], while they are so unique and the potential accident consequences are so unacceptable that a direct inference from historical experience is not possible. Despite the declared allegiance to the use of PRA, from the practical perspective, NASA's approach to safety remains strong. In accordance with PRA procedures, safety is measured by risk defined as a comprehensive set of accident scenarios along with their respective likelihoods and consequences. Two obvious challenges arise: to ensure that this scenario set is indeed comprehensive and to evaluate the likelihoods. The former challenge is certainly a daunting one, but apparently manageable by NASA quite successfully – the loss of both Orbiters is attributed to the failures whose possibility was conjectured beforehand. In contrast, the record of the Agency's treatment of likelihood evaluation is somewhat more mixed. As argued in the context of the *Challenger's* accident [7], NASA reliance on the critical item list (CIL) and associated disregard of the importance of likelihood has deep historical roots. The only way CIL accounts for different likelihoods of events is by differentiating the levels of redundancy. Obviously, this provides a very coarse resolution for addressing the likelihood, as a redundancy can be easily defeated if it involves events with a relatively high likelihood, while a single-point-failure can be extremely unlikely. While risk matrices are currently employed, their quantitative interpretation is far from straightforward. Furthermore, the meaning of likelihood in a risk matrix might be interpreted not in a probabilistic sense, but be related instead to the ease with which the accident scenario can be averted (i.e., mitigation options). The latter is obviously very important yet unrelated to the likelihood of occurrence. This reluctance to employ likelihood in decision-making process can be partially attributed to the uncertainty inherent in the probabilistic predictions: high sensitivity to "chance events" that provide external disturbances to the system necessitate statistical characterization, and this characterization is often based on a poor sampling base unless the relevant accidents occur frequently enough. This is counterintuitive to engineers' mind set with its fundamental reliance on deterministic causality. Contrary to the traditional engineering experience, there is no immediate feedback provided by implementation – a well-designed system can fail due to unfortunate circumstances, while a serious design flaw may remain latent for a very long time.

As a result, verifying the prediction can be extremely difficult. A system pronounced safe by the analysis can fail due to:

i. Statistical variation that complies with correctly predicted statistical characteristics of the system: "bad luck" corresponding to aleatory (irreducible) uncertainty.

ii. Uncertainties in predicting statistical characteristics of the systems within a chosen predictive model (PRA aims at quantification of these uncertainties).

iii. Incorrect modeling ("unknown unknowns"): missed failure modes, wrong assumptions, etc.

It is important to distinguish among these three sources to facilitate a meaningful decision-making process, but this task if far from trivial. In accordance with PRA procedures written for NASA practitioners [5], an explicit probabilistic treatment of epistemic (i.e., caused by the lack of knowledge) uncertainty is recommended; this corresponds to the second source (ii) in the provided above classification. This implies the use of probabilistic distributions instead of point estimates for the statistical parameters of the relevance to the risk assessment events. However, no data might be available to infer the type and properties of these distributions, while the final results are usually extremely sensitive to this information. Often, only ranges of possible values for the parameters might be available (e.g., based on the expert opinion solicitation), but not the distribution within those ranges. To address this problem the use of so-called Generalized Information Theory (GIT) is advocated [8].

Interval-based uncertainty modeling. GIT has received significant attention of researchers in recent years and it encompasses possibility theory, Demster-Shafer evidence theory, as well as fuzzy set theory. A comprehensive taxonomy of uncertainty modeling is provided in [9].Within the GIT framework, interval-based calculations are conducted to arrive at lower bound (referred to as belief and necessity in evidence and possibility theories, respectively) and the upper bound (referred to as plausibility and possibility in evidence and possibility theories, respectively) of a risk measure as opposed to a traditional probability approach that provides a single estimate for this measure. Furthermore, a strict "all-or-nothing" membership of classical set theory can be relaxed by means of fuzzy sets [10], where for a set $A \subset X$ a continuous measure of the set membership $\mu_A : X \rightarrow [0,1]$ is introduced to reflect intermediate relationships (whereas only extreme values 0 and 1 are realized in classical set theory). For any value $\alpha \in [0,1]$ a so-called α-cut defined as ${}^{\alpha}A \equiv \{x \in X \mid \mu_A(x) \geq \alpha\}$ represents a classical (so-called "crisp" set) that corresponds to selecting α as a threshold for the inclusion into the set membership. By varying α one can form a nested family of sets ${}^{\alpha}A \subseteq {}^{\beta}A$ when$\alpha > \beta$. Applying these concepts to risk assessment, one can consider a family of nested family of intervals that represent range of values supported by evidential data, where α-cuts generalize the classical notion of confidence intervals.

Risk Modeling. For mass produced systems, such as cars or commercial airplanes, a direct operational experience usually provides sufficient statistics to significantly reduce the influence of both (ii) and (iii), thus facilitating construction of high-fidelity predictive models. On the other hand, for one-of-a-kind systems, distinct characterization of these sources of uncertainty presents formidable challenges. Two main approaches could be identified in addressing these challenges: holistic (unstructured) and system (structured or analytical) approaches. The former treats the system as a whole, while the latter relies on decomposing the catastrophic event into a set of more elementary events and conditions. Brief descriptions of each approach as well as their advantages and drawbacks are provided below:

Unstructured approach (black box point of view): Assessing behavior of a system as a single entity provides obvious advantages of simplicity with only few parameters determining system safety. If the relevant data is available, quantifying risk and estimating parametric uncertainty (i.e., type (ii)) is fairly straightforward. The simplest version of this approach corresponds to observed reliability [11] and is based solely on past experience of the system under consideration. Due to the scarcity of system-specific data, selecting events that are significantly similar to the studied catastrophic event presents the following dilemma: a relatively loose similarity selection criterion poses the problem of accounting for dissimilarity (such as between wire-to-wire "smart" short vs. wire-to-ground shorts); on the other hand, a more strict similarity criterion leads to a small sampling pool, with resulting difficulties for any meaningful statistical inference. Effectively, resolving this dilemma requires a certain degree of event decomposition, but unlike the system approach described below, system approach this decomposition is conducted informally based on qualitative arguments. Even assuming that this separation of all historical data into relevant (i.e., sufficiently similar) and irrelevant sets is conducted superbly, in most of the practical cases the very need of providing a crisp threshold inevitably results in overestimating the relevance of included events (since they rarely are identical to the modeled accidental event) while discarding the information associated with the excluded events completely. Here it is appropriate to note that the Space Shuttle Program (SSP) has relied on this approach, and their selection of only two wire-to-wire "smart" shorts as relevant events provides a good example of the described problem. A more flexible treatment would allow for a continuous measure of relevance, e.g., varying from 0 (totally irrelevant) to 1 (identical), with the contribution to the final analysis apportioned in accordance with this measure of relevance. If such a measure is provided, fuzzy set classification [10] provides natural means to account for it. The lack of system-specific data can be partially compensated by means of Bayesian analysis, which is discussed below.

If a failure of a complex repairable system, such as the SSP, is considered without any formal event decomposition, then the stochastic point processes are usually used to describe the failure occurrences [12]. The most common model corresponds to a Homogeneous Poisson Process (HPP) that describes a situation where, upon failure, the system is immediately restored to as-good-as-new condition (perfect repair). Furthermore, each consecutive failure has the same statistical characteristics as the previous one, implying that the system neither deteriorates (ages) nor improves with time. Under this conditions the probability of occurrence of n failures in time segment [0,t] is

$$p(n,t) = P(X = n) = \frac{(\lambda t)^n \exp(-\lambda t)}{n!}$$

HPP can be considered as a natural generalization to repairable systems of exponential (constant) failure rate used for non-repairable systems, as the time between any two consecutive failures follows the same exponential distribution. On the other hand, non-homogeneous Poisson process (NHPP) can account for aging (which can be manifested in less-than-perfect repair).

System (analytic) approach (white box point of view): decomposing a complex event into a set of more elementary events and conditions is usually more involved when compared to the unstructured modeling, but the benefits can be enormous. The following main advantages can be identified:

- A unique system is usually constructed of sub-system or components that are more standard, so their behavior can be better statistically characterized based on the previous experience from other systems.
- The “fuzzy” issue of similarity of different complex events (see the discussion above) can be more easily quantified by representing them as chains of simple events and identifying shared links in those chains. For example, a chain of event leading to a wire-to-wire “smart” short can be meaningfully compared to a wire-to-ground short by identifying additional conditions required for the former.
- Testing at the subsystem or component level is easier to conduct and is usually more extensive than the system-level testing. This leads to inherently less reliable system-specific data for behavior of a system as a whole, as opposed to behavior of its parts. This trend becomes even more pronounced for very complex system: the SSP was the first American spacecraft that was not flight-tested as whole system [13].
- If the absence of “hard” data experts’ opinions on the likelihood of events can be solicited and relied upon. Experts’ estimates are prone to systematic and significant biases [14]. Event decomposition is recognized as one of the most effective methods to reduce this bias [15]. This is particularly true when dealing with rare events, as humans (including experts) have great difficulties in assessing very small probabilities. Elementary events are more likely to occur and therefore can be better estimated than a directly estimated complex event composed of a sequence of those elementary events.
- PRA is only one of several factors used in a decision-making process. Another important factor is historical experience with the system. By using a holistic approach to PRA these two factors become highly correlated, effectively replicating one another. On the other hand, event decomposition leads to more independent results that often provide a usefully distinct perspective at the problem at hand.
- Event decomposition aids identifying weak links in the design by providing consequent sensitivity studies which facilitates selection of effective mitigation options.

By far the most common method of system failure analysis (and a cornerstone of PRA procedure) is Fault Tree Analysis (FTA), which was introduced in the early 1960s [16,17]. In standard form, FTA relies on two logical “gates” (“AND” and “OR”) to combine “basic events” (i.e., leaves of the tree) into the “top-level event” (root of the tree). This allows evaluating the probability of top-level event based on given probabilities for basic events. Figure C-2 depicts a simple fault tree with three basic events (denoted as circles) combined into a top-level event by means of a single “AND” gate (note the flat bottom of the symbol for the gate). Figure C-8 presents a more complex fault tree (a detailed description of this fault tree is provided in the later chapters of this Appendix), where the top-level event is an “OR” gate (thus a concave bottom of the corresponding symbol). In addition to the “AND” gate (WWSHORT), the fault tree contains so-called transfer gates (denoted in Figure C-8 as triangles, gates DARLINGTON and WWCONTACT). Transfer gates are purely a means to break a big tree into smaller ones that allow hierarchical representation of fault trees (e.g., gate DARLINGTON is expanded in Figure C-12, which represents the fifth page of the fault tree: note the reference to that page underneath the gate symbol and gate WWCONTACT is similarly expanded in Figure C-9, which is the second page of the fault tree). The main advantage of FTA is its ability to focus on the top-level event of interest, rather than describe all possible states of the system. For example, the system modeled in Figure C-2 can have $2^3 = 8$ possible distinct states if all three basic events can occur independently (each event either occurs or does not). However, in FTA probability of only one state is considered relevant and calculated (corresponding to all three basic events occurring simultaneously). On the other hand, state-space based methods such as Markov chains and Petri nets model all possible system states, which makes them susceptible to the so-called "space explosion" when the size of the model grows exponentially with the number of elementary events effectively precluding all but the smallest models (however, there is a way to circumvent this problem for Petri nets, as discussed below).

One of the main disadvantages of the FTA stems from its reliance on independence among the basic events. Modeling-dependent events can be critical for understanding the system's behavior in its own right, but the situation is further compounded by the binary nature of FTA as it complicates modeling a very common situation when there are more than two possible states. To illustrate this point, let us consider a simple situation where a transistor can be in one of three possible states: *operating, shorted,* or *opened*. Let us assume that the short of this transistor can lead to a condition A, while the opening of the same transistor can lead to a condition B. Let us further assume that simultaneous occurrence of both A and B (represented by two branches connected by gate "AND") leads to a catastrophic event C. Since this transistor cannot be both shorted and opened at the same time, C cannot occur solely due to the failure of this transistor, but it is hard to account for this using FTA. Obviously, if the transistor is the sole source of both events A and B, one could just eliminate the whole branch (which in practical situations can be not as trivial as it seems since FTA construction encourages step-by-step thinking). However, if either A or B can be caused by some other events, then the branch cannot be eliminated altogether and modeling using FTA would lead to completely erroneous results.

As described in [5] (Section 6), fault trees also have limited capabilities in modeling complex dynamic scenarios where the timing of individual events is critical for evaluation of the probability of failure. A standard PRA practice [4] is to model temporal aspects of the failure scenarios using event trees, with fault trees used to model (static) logical inter-relationship for so-called pivotal events. However, the dynamic nature of the basic events for fault trees often needs to be modeled as well. While numerical values for basic events can be provided in terms of failure rates, those rates are consequently integrated over the duration of the mission (or the appropriate portion thereof) to yield the total probability of this event occurring during a given mission. Alternatively, the total probabilities for basic events are input directly. Regardless of how those total probabilities are obtained, they are combined using Boolean logic to render the probability of the top-level event.

In contrast to FTA, Bayesian (belief) networks (BN or BBN) provide a very efficient means of modeling dependency and are extensively used in the context of artificial intelligence. Recently their application to system reliability started to attract serious attention as a possible and more flexible alternative to FTA [18]. Events in BBN are represented by nodes which are connected into a directed graph. The direction of each connection indicates a parent-child relationship (connection goes from a parent to a child). No cycles (loops) are allowed. Nodes without parents are referred to as root nodes (and their marginal probabilities are specified for each value at the node, the latter is not being limited to binary values). Conditional probabilities are specified for non-root nodes for each possible combination of its parent node values. Continuing with the transistor example, one can observe how the described above difficulty with the FTA is trivially resolved using BBN (see Figure C-1).

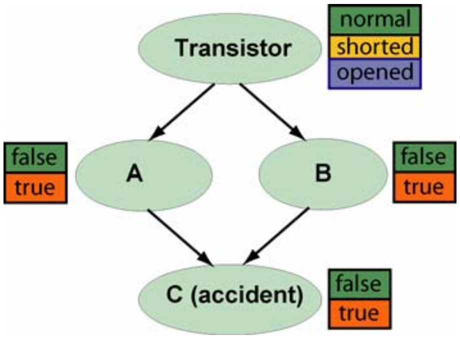


Figure C-1. A Simple Bayesian Belief Network for a Transistor with Three Possible States

Describing dependency in a local fashion allows avoiding a full description of the state space, and any FT model can be recast into a BBN. Additional features as compared to FTA include:

- Multi-state variables
- Sequentially dependent failures
- Probabilistic ("noisy") gates that provide a convenient means to model uncertainty: rather than stating that occurrence of events A and B will lead to event C (deterministic causality is expressed by standard "AND" gate), a noisy "AND" gate will specify the probability of C occurring conditioned on the occurrence (and, importantly, non-occurrence) of A and B
- Meaningful measures of criticality for a root node (i.e., basic event) based on evaluating posterior probability of the node given the system failure (see the section of Bayesian Methods on Bayesian updating below)

The role of BBN modeling in system reliability is likely to increase in the future. However, both FTA and BBN rely on static causality, which explains the absence of loops describing feedback mechanisms and limits their capabilities to model dynamic scenarios including repairs and system's reconfiguration in response to changing circumstances (an increasingly important feature of complex systems). In such situations, one has to resort to state-space based models that provide means to evaluate transitions among the system's states.

Markov chains are the simplest and most common state-space modeling technique with each possible system state denoted by a circle and directed arcs indicating transitions between states. These transitions are characterized by a single constant parameter corresponding to the transition rate (although multi-phase modeling is possible with the constants changing between phases). Figure C-3B shows a simple example of a Markov chain. Two important drawbacks of this technique can be identified:

- State-space explosion: the size of Markov chain models grows exponentially with the number of components/events. As a result, only a very small number of components/events can be modeled within a single model.
- The constant transition rate reflects the so-called memory-less property of Markov models where the future depends only on the present (and not on the past) and corresponds to transitions occurring in accordance with exponential distribution. Modeling of systems that either age or improve with time requires introduction of auxiliary system states, thus further increasing the model size.

Stochastic Petri Nets (SPN) provides an attractive alternative of Markov chains as they address both of these issues [19, 20]. Figure C-3C depicts SPN model for wire damage. Petri nets are directed graphs with two disjoint types of nodes: places (denoted as circles) and transitions (denoted as rectangles). A directed arc connects a place to a transition (an input arc) or a transition to a place (an output arc). The places connected to a given transition by input or output arcs are called the input or output places, respectively, for this transition. Each place can be assigned a non-negative number of tokens (denoted as small circles). A combined token assignment for all the places in the model fully characterizes the system state, and is referred to as the model's marking. Changes in the system state are reflected in token movements, which are in turn facilitated by the so-called "firing" of transitions. For a transition to be fired it must be enabled for a specified amount of time. A transition can be enabled if all its input places have tokens. Other requirements that are functions of marking can be present as well. Transitions can be classified in accordance with the specification of the delay between enabling of a transition and its firing; such a delay can be absent (an immediate transition, denoted with a thin bar), deterministic, or sampled from a given distribution (stochastic). Timed transitions (both stochastically distributed and deterministic) are denoted with a solid rectangle. Upon firing, a transition removes a token from its input place and deposits a token to its output place.

The following differences between Markov chains and SPN are noted:

- In Markov chains each circle corresponds to the state of the system as a whole. Marking provides the same functionality for SPN, where each token location can correspond to a more elementary event (or component state). As a result the system state is implied in SPN which results in much more compact description of large systems, since there is no need to explicitly enumerate all the possible permutations of elementary states. Obviously, when only one token is used (as in Figure C-3C then its location denotes the system as a whole as in Markov chain). For example, one could refine the modeling by distinguishing two types of wires: those located in the high-traffic area (and therefore prone to induced failures, but also easily accessible) and those in the low-traffic area. Then each of these types can be represented by a token and the model would have two tokens instead of one without the need to explicitly extend the state-space (as required to represent the same model using Markov chains).

- Transitions in SPNs are not limited by constant-rate assumption, so general distributions (such as Weibull or Lognornal) can be directly accommodated.

Bayesian Methods

With the availability of power computing resources, computationally-intensive Bayesian statistical methods become more and more popular [21] and these techniques play an important role in conducting a PRA [4,5]. The Bayesian approach to statistical inference relies on the existence of a so-called prior distribution for the modeling parameters $P\{\theta\}$, which reflects the knowledge about θ before current data is taken into consideration. This knowledge about θ can then be updated given the current data σ to obtain the so-called posterior distribution:

$$P\{\theta \mid \sigma\} = \frac{P\{\sigma \mid \theta) \bullet P\{\theta\}}{\int P\{\sigma \mid \theta) \bullet P\{\theta\} d\theta}$$

Based on this posterior estimate, a predictive distribution of a future observation $\tilde{\sigma}$ can be calculated:

$$P\{\tilde{\sigma} \mid \sigma\} = \int P\{\tilde{\sigma} \mid \theta) \bullet P\{\theta \mid \sigma\} d\theta$$

In contrast to the maximum likelihood method, this representation directly accounts for uncertainty in the estimation of the modeling parameter $\tilde{\theta}$ (since it is specified as a distribution). In the context of reliability and safety modeling, the most common application of the Bayesian technique is merging heterogeneous sources of data. The simplest (and possibly the least controversial) example of such situation can be described as follows:

A mass produced device (i.e., transistor) has a well established statistical characterization of failure distribution that is used as a prior estimate. Next, the device is tested for defects and the data on the reliability of the test prediction to be correct is provided (i.e., avoiding false positive or negative). Then, Bayesian updating provides a consistent means to combine the results and, prior to obtaining posterior estimate of the probability, that the device is faulty. This concept is generalized to treat generic data about similar entities as prior estimates and merging it with (usually sparse) system-specific data. While theoretically this approach provides a means to compensate for the lack of system-specific data, both at the component and system level, the final results are very sensitive to the external data, and the construction of a good prior estimate is crucial. However, at the system level, this presents a formidable challenge due to the effective uniqueness of each complex system. Samandar Roshan-Zamir (SAIC) used this approach by constructing a prior estimate based on civil transport aircraft data. The results do not inspire high confidence, as they provide prior failure rates that are almost two magnitudes lower than the Shuttle-specific data. It is reasonable to suggest that rates, if anything, could be higher (due to less strict aircraft maintenance practices and the harsher environment seen by aircraft wiring). This Bayesian approach was abandoned in a recent SAIC updated report in lieu of the observed reliability approach. This does not necessarily imply that the approach is not feasible, but a rigorous quantification of both differences and similarities among the systems must be conducted. Analysis of FAA data, provided in Appendix G of this report, provides first steps in this direction.

Critique of the SAIC Point Estimate

The point estimate ($9.05E^{-6}$) relies on two failures. A constant failure rate or, equivalently, a Homogeneous Poisson process is assumed. A standard procedure for providing confidence intervals bounds this estimate within [$1.096E^{-6}$, $2.521E^{-5}$] for 95% confidence. However, the following serious potential drawbacks are identified:

- Aging was not considered in the analysis. Obviously, two failures do not provide enough information to support or reject any presence of aging; however, it is important to recognize that the absence of aging is a non-conservative assumption. Appendix G of this report provides a strong case for significant effects of aging and, as shown below, the presence of aging significantly affects risk estimates.
- This calculation uses the fact that RCS signal wires constitute approximately 0.005 fraction of all Orbiter wires. By definition, a wire-to-wire "smart" short implies at least TWO wires are in contact. Therefore, it should be assumed that the probability that at least one of the two wires is not 0.005, but rather 0.00995, unless a more detailed classification of wires is provided. The point estimate changes to $1.801E^{-5}$ with a 95% confidence interval [$2.181E^{-6}$, $5.017E^{-5}$]. Moreover, there is no certainty that only two wires participate in a short. If more wires are involved in a short, the probability needs to be adjusted appropriately. Out of two events that were considered relevant, the first event damaged six wires. If we consider those events representative (that is a wire short on average involves four wires, corresponding values practically double, resulting in a point estimate of $3.602E^{-5}$ with a 95% confidence interval [$4.362E^{-6}$, $1.003E^{-4}$].
- The issue of the delectability of wire-to-wire "smart" shorts (especially intermittent ones) remains a big unknown, as it is recognized that ALL shorts reported in PRACA are due to the observed malfunctioning of some equipment. It is reasonable to assume that some intermittent shorts went unnoticed (which might explain the problem discussed in the previous bullet). However, such shorts are capable of causing the catastrophic event.

Critique of the AMES Report

The PRA conducted by Kushik Datta (NASA Ames) is discussed.

Review of Assumptions. A system level approach was used in the NASA Ames PRA with the Fault Tree (FT) constructed to evaluate the influence of several failure modes. While the study itself was quite detailed, a few key assumptions are listed below that are sufficient to capture the final numerical results with good precision:

- A number of exposed conductors, or significant damages to wires, were observed during the down period of OV-102 and OV-103. For each Orbiter, the number was assumed to be SD = 470, which constituted about 10% of total wire damage incidents observed. These numbers were provided to K. Datta by P. Krause.
- This observed wire damage was assumed to follow the HPP that is proportional to the wire length. Corresponding failure rate per feet of wires was calculated based on the following formula:

  $$\lambda = \frac{SD(1 - f_i)}{L_{wires}N_f}$$

  where L_{wires} is the total length of wires in the Orbiter in feet, f_i = 0.25 fraction of wires inspected for damage in every turnaround, and N_f is the number of flights before major inspection of OV-102.

- Two major mechanisms contributed to the final numbers: chafing of the wires and carbonization of wires via arcing. The relative frequency of these failures as compared to SD was inferred from PRACA reports: from a total of 1,514 reports of wire damage, there were 162 reports of chafed wires and 1 report of arcing. Therefore, D_{chaf}= 162 × SD/1514 = 50 and arc tracking Darc=0.31.
- Given the estimated length of control wires $L_{control}$= 4000 ft and power wires in RJD bundles L_{power} = 40000 ft, the rate of occurrences of chafing of a control wire $\lambda_{ch} = \lambda\, \underline{D_{chaf}}\, L_{control} = 7.284 \text{ x } 10^{-3}$ and arcing of a SD and of a power wire is estimated $\lambda ar\ \underline{\lambda D_{ar}}\ L_{power} = 4.516\ 10^{-4}$.
- Total probability for a single mission of two types of events is then calculated: at least one chafing of a control wire in a RJD bundle $P_{chaf} = 1 - \exp(-\lambda_{ch}) = 7.26 \times 10^{-3}$ and, similarly, that at least one arcing takes place for a power wire in an RJD bundle $P_{arc} = 1 - \exp(-\lambda ar) = 4.52 \times 10^{-4}$.
- Additional conditional probabilities are introduced: P_{multi} = 0.1: given that a signal wire is chafed, there is a probability that a neighboring wire is chafed as well. (The value 0.1 is taken as a generic value of a common cause factor), and P_{SP} = 0.5, corresponding to the fact that given a multiple chafing, the adjacent wire is a power one (a better estimate of this probability is not available). Probability of the wire-to-wire "smart" short due to chafing is $P_{wc} = P_{arc}\, P_{multi}\, P_{SP} = 3.63 \times 10^{-4}$.
- Combining arcing and chafing failure modes yields $P_{tot} = 1 - (1 - P_{wc})(1 - P_{arc}) = 8.148 \times 10^{-4}$. The inclusion of all other modes changes the total number to 8.3867×10^{-4}, or less than 3% difference, so the other modes are basically negligible.
- It is assumed that after 1999 events, there was a 6-fold improvement in maintenance that resulted in a 6-fold decrease in wire damage. This factor was obtained by observing an average of a 6-fold increase of the reported damage in 1999 followed by the rate of reporting that is of the same magnitude as pre-1999 years. The conclusion was made that six times better detection of damaged wires was equivalent to a 6-fold decrease in the underlying failure rates. This led to the final number $P_{fin} = 1.4 \times 10^{-4}$.

Discussion. The Ames study was considered overly conservative, which was the primary reason for its results to be ultimately dismissed by the Shuttle program. It is important to mention some interesting features of this analysis that can be questioned, and how the changes in these assumptions alter the final numbers:

- It is assumed that initially there was no damage to wires, and this damage uniformly accumulated during 26 flights. The difficulty comes from the need to reconcile the issues of repairable and non-repairable systems. Strictly speaking, a HPP used to model wire damage is defined for repairable systems: applicability of HPP implies that each occurring failure is repaired, and the system is restored to its original configuration i.e., the old damage is removed. On the other hand, the Ames report uses the assumption of the linear damage accumulation, which can only be made compatible with HPP if a different time scale is considered. The latter time scale is equal to 26 flights: it is assumed that after OMDP in 1999 ALL the damage was detected and removed. In addition to the issue of detectability (which cannot be 100%), the model does not account for regular maintenance.
- Damaged wire does not necessarily cause an immediate short. Use of the larger time scale effectively averages the occurrences of wire shorts over 26 flights without addressing potential inequalities in risks between the flights right after and before OMDP (it seems reasonable to assume that the risk is lowest right after OMDP as the number of damages wires is the lowest).
- There was no distinction made as to when during the turn-around cycle the failure occurred. This is a very conservative assumption, that can be easily replaced with a more realistic assumption that the damage is permanent and immediately detected, which leads to a simple calculation of a correction factor by dividing the docking time by the total power-on time during one cycle (based on the values provided in the SAIC report, this would yield $P_{firstdoc} = 0.090546$).
- It is not clear why f_i is introduced: whatever the percentage of the detection was per turnaround, if anything, its effect should be the opposite (as it increases the total number of damage accumulated between two OMDPs).
- A 6-fold improvement in the rates of damage cannot be assumed.
- As shown in Appendix G, the no-aging assumption might be too optimistic.

Present Approach

Justification for a Dynamic Model for Wire Damage

The goal of the constructed numerical model is to provide an estimate of the probability of failure occurring during a single mission, and for the duration of the program

A notional FTA for a short in a RJD bundle is shown in Figure C-2. Here, Event A characterizes the likelihood of relevant wire damage in the RJD bundle, while Events S and D provide additional conditions for the short to occur. S is a (composite) representation of static events (the conditions either exist or they don't): power and signal wires are next to each other or not; given a current spike, a fuse blows or doesn't, etc. In contrast, D is a (composite) representation of a dynamic event that can occur continuously in time and, therefore, should be characterized by the rate of occurrence.

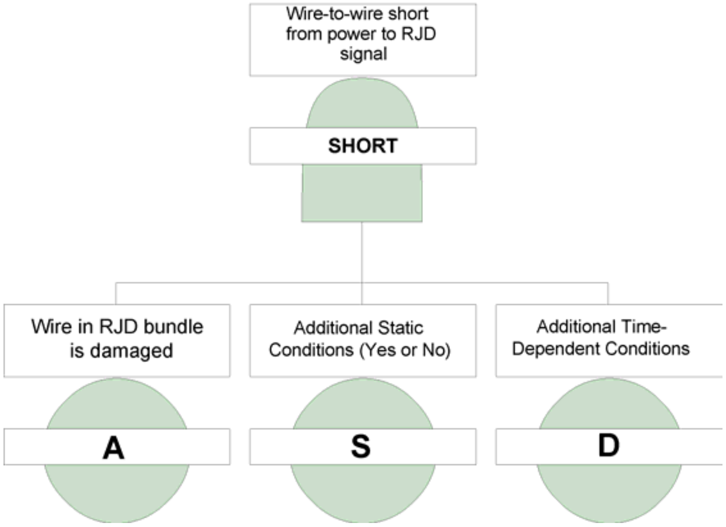

Wire-to-wire short from power to RJD signal
SHORT
Wire in RJD bundle is damaged
Additional Static Conditions (Yes or No)
Additional Time-Dependent Conditions
A
S
D

Figure C-2. Notional Fault Tree for a short in RJD bundle

It is realistic to assume that Event A reflects the *total* amount of damaged wires, while events of Type D will provide a dynamic representation of the additional processes required for a short to occur. In the following text, a type of each event is specified for clarity.

Let us also note the subtlety of properly accounting for the possibility of having more than one instance of damaged wires in a RJD bundle. This is a relevant issue assuming the Ames report numbers for SD, N_{SD}= 470 leads to the expected value of SD for signal wires in the RJD bundle to be F_{control}=2.374. While one can calculate a probability that at least one instance of damaged wires exist in the RJD bundle, the use of that value in the fault tree will lead to underestimating the probability of the top-level event. Instead, frequency of occurrence should be used. To take advantage of standard fault tree software tools that require probability values as inputs (which obviously must be less than 1), it is convenient to appropriately adjust the values of two events comprising the same AND gate. For example, if the proper values for events A and C in Figure C-2 are $Q_A = 2.374$ and $Q_C = 0.02$, then by introducing an auxiliary factor $m = 10$, one can provide valid entries to the fault tree that do not alter the probability of the top level event: $P_A = \frac{Q_A}{m} = 0.2374$ and $P_C = mQ_C = 0.2$.

Damage Accumulation (Aging)

Modeling of the Space Shuttle wiring presents a particular challenge due to the difficulties of applying conventional notions of repairable systems. In particular, an assumption of HPP implies that upon each failure the system is repaired and returned to “as new” condition. One can hardly claim that wire inspections lead to a 100% success in repairing wires, so the definitions of “as new” and “absence of aging” must be defined with caution.

It is quite reasonable to assume that the probability of wire shorts is proportional to the total amount of damaged wires present in the Shuttle at any point in time. A simplified schematic of the associated processes is shown in Figure C-3. It is convenient to use a single shuttle turn-around as a unit time. Then, λ_1 is defined as the transition rate for the wires that “naturally” degrade over time; λ_2 corresponds to the maintenance induced damage rate (with $\lambda = \lambda_1 + \lambda_2$ corresponding to the total damage rate, while μ denotes the rate of detected and repaired wires).

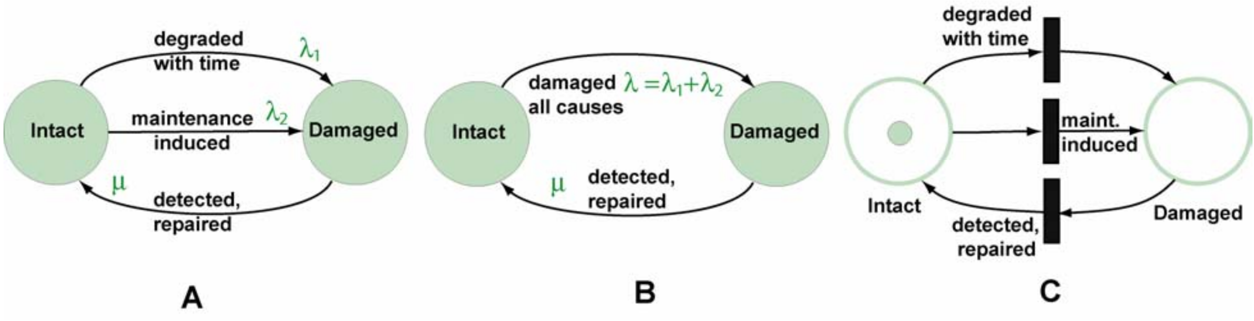


Figure C-3. Sources of changes in the total wire damage (A), corresponding Markov chain (B) and Stochastic Petri Net (C)

Most of the factors that are contributing to the wire damage in the Orbiter are discrete events with respect to time. However, it is convenient to represent routine life cycle of an Orbiter using continuous time. Only the last baseline maintenance and the 1999 stand-downs are explicitly modeled as discrete events due to their significance and non-recurring nature. Let us denote the total amount of relevant damaged wires with N (the relevant categories of damage include exposed and damaged conductor). Noting that damage is measured in instances (discrete), while the wire is measured in unit of length (continuous), we may choose the unit of length that is small enough to neglect the possibility of having more than one damage per unit length (e.g., feet as opposed to miles). Then we can introduce a non-dimensional quantity, $y(t) = \frac{N(t)}{N_{tot}}$, where N_{tot} is the total amount of wire in the chosen units which effectively measures the probability that a given wire segment of unit length contains damage. The equation for $y(t)$ has the following form:

$$\frac{dy(t)}{dt} = \left(1 - y\right)\left(\lambda_1(t) + \lambda_2(t)\right) - y\mu(t)$$

The equation above is a first order differential equation so, for any time segment, an initial condition needs to be specified. Three time segments are used (as appropriate):

1. Initial installation, stand down (1999).
2. Stand down (1999), the last OMDP.
3. The last OMDP, future operations.

Initially, it is reasonable to avoid any differentiation among the wires, with understanding that further refinement of the model is possible with the rates being different for various locations (depending on the accessibility of the wires).

If all those rates do not change with time, the corresponding process can be represented as a Markov chain where λ_1 and λ_2 are combined into a single transitional rate (see Figure C-3B). In contrast, increasing with time λ_1 (t) corresponds to the "wear-out" portion of the bath-tub curve, which for non-reparable components (such as individual wires) can be modeled using Weibull distribution with the shape parameter $\kappa > 1$. Such modeling can be implemented using Stochastic Petri Nets as depicted in Figure C-3C.

It is important to note that even if λ_1 is constant (i.e., $\kappa = 1$), the total amount of damaged wires (and therefore the probability of wire shorts) can still increase in time. For example, in the situation where $\mu = 0$ (i.e., for wires that are not accessible), damaged wires will certainly accumulate (albeit possibly at a slow rate).

To account for events that occurred in 1999, two-phase modeling can be implemented. At the beginning of the second phase, a significant amount of wire damage was repaired, and consequently λ_2 has been significantly reduced (Ames report cites a 100-fold decrease in the induced damage due to new procedures), while μ is increased (Ames report assumes 6-fold increase of delectability). It is reasonable to suggest that λ_1 remains unchanged since no changes in operating condition and storage environment can be identified.

Wire-to-Wire "Smart" Short Model

In constructing a model for evolution of wire damage, an attempt was made to attain a balance between fidelity and simplicity. The following parameters are considered to be an input to the model:

1. INITIAL: Q_1 fraction of all damaged wires (existing during the last OMDP) that were introduced during initial installation.
2. DETECTBEFORE: Q_2 average effectiveness of inspections before 1999 (per turn-around) includes prior OMDP.
3. DETECTMAJOR: Q_3 measures effectiveness of the last OMDP: the fraction of detected significant damage (damaged and exposed conductor) to the total amount of significant damage existing in the Orbiter at the time of OMDP.
4. DETECTAFTER: Q_4 effectiveness of routine inspections after 1999.
5. WEIBULL: Q_5 Weibull shape factor for all wire damage accumulation excluding maintenance-induced damage.
6. MAINTCAUSE: Q_6 fraction of damage accruing in the Orbiter that is maintenance-induced (as opposed to all other sources of accumulated damage). Please note that this parameter is related to damage accumulation that occurs after initial installation (and therefore is independent on parameter Q_1).
7. MAINTIMPROVE: Q_7 fraction of maintenance-induced damage after 1999 as compared to pre-1999 procedures. This parameter is an inverse of the maintenance improvement factor that quantifies the amount of induced damage.

The list of numerical value-related parameters is provided in Table C-1.

Once parameters Q_1-Q_7 are defined, the model is constructed as follows:

- Amount of relevant significant damage number of instances of (damaged and exposed conductor), N_e is determined for the last OMDP. The total amount of damage present in the system during that OMDP is calculated as:

$$N = \frac{Ne}{Q_3}$$

- Initial amount of damage is evaluated: $N_i = Q_1 N_t$. This value provides the initial condition for the damage evolution for the first time segment.
- Repair rate μ(t) for each time segment must be consistent with the assumed levels of detection, as the absolute values of the "outflow" of damage (that is, the amount of removed damage in accordance with the model) should correspond to the observed amount of detected significant damage.
- Let us assume that $\lambda_1(t)$ follows Weibull distribution:

  $$\lambda_1(t) = \frac{\kappa t^{\kappa-1}}{\theta^{\kappa}}$$

  here Q5 provides κ. Furthermore, given Q6 (the ratio of induced and "natural" failures before 1999), one can express λ_2 in terms of θ. Finally Q7 allows to express changes in λ_2 after 1999. Therefore, θ uniquely defines failure rates for all time segments. Therefore, the solution of the differential equation with θ as a parameter presents an equation $N(t_{OMDP}, \theta) = N_e$ which can be solved to determine θ.

The time history for OV-103 of exposed and damaged conductors is shown in Figure C-4 for 35 flights, where stand-down takes place after 26 flights and major inspection (OMDP) takes place after 30 flights. Three curves correspond to different values of Q_4 from Table C-1. Based on the preliminary comparison with the historical data, Q_4=0.1 appears to be reasonable. Note that for OV-102, OMDP coincided with the stand-down period. The estimate directly uses exposed and damaged conductors as the relevant damage. The fault tree is constructed for the 33rd flight of OV-103. Figure C-4 shows a somewhat counter-intuitive trend: after 1999, the amount of damage decreases due to routine maintenance, which seems to obviate any need for OMDP. Based on the investigation of PRACA data for OV-103 (see Appendix G), one can conclude that values Q5 and Q6 from Table C-1 can be significantly different from what was assumed initially. Figure C-5 demonstrates the changes in total damage for 33rd and 36th flights with all the parameters kept the same, but varying Q5 (in accordance with Appendix G, the value 2.2 can be suggested).

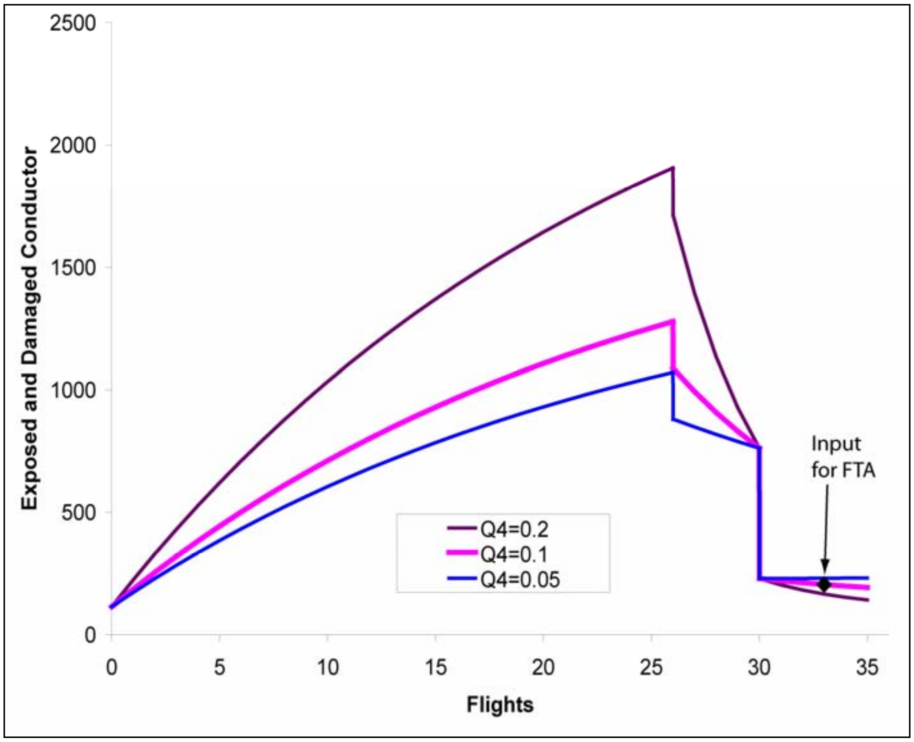


Figure C-4. History of Total Number of Wire Significant Damage (based on the parameters given in Table C-1)

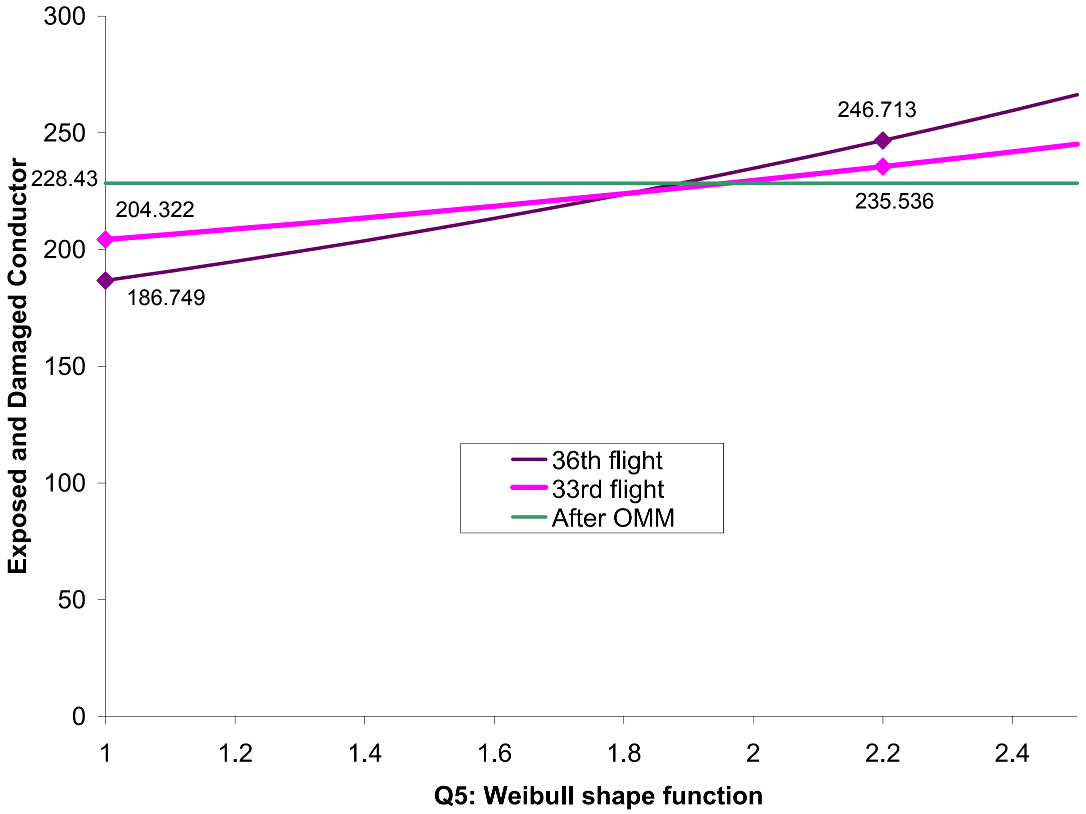


Figure C-5. Sensitivity to Weibull Shape Function: Q6=0.9

It can be observed that for these other parameter values, the sensitivity with respect to Weibull shape parameter is minor. The fault tree depicted in Figures C-8 through C-14 is based on the total amount of significant damage being 204.322 (see Table C-2 and also left of Figure C-5). It must be noted that the top-level value is almost directly proportional to the amount of significant damage. However, the situation is drastically changing if we also take advantage of the data provided in Appendix G with respect to the ratio of induced damage. Therein, the statistics shows that the ratio of such damage can be as low as 0.175. Taken into account Q1, one can conclude that Q6 = 0.20588. Figure C-6 demonstrates the results of dynamic wire damage model: the amount of damage is doubled for the 33rd flight and tripled for the 36th flight, causing similar magnitude of changes to top-level event estimates (under this scenario the total value of risk for 33rd flight becomes 3.26 10^{-4}).

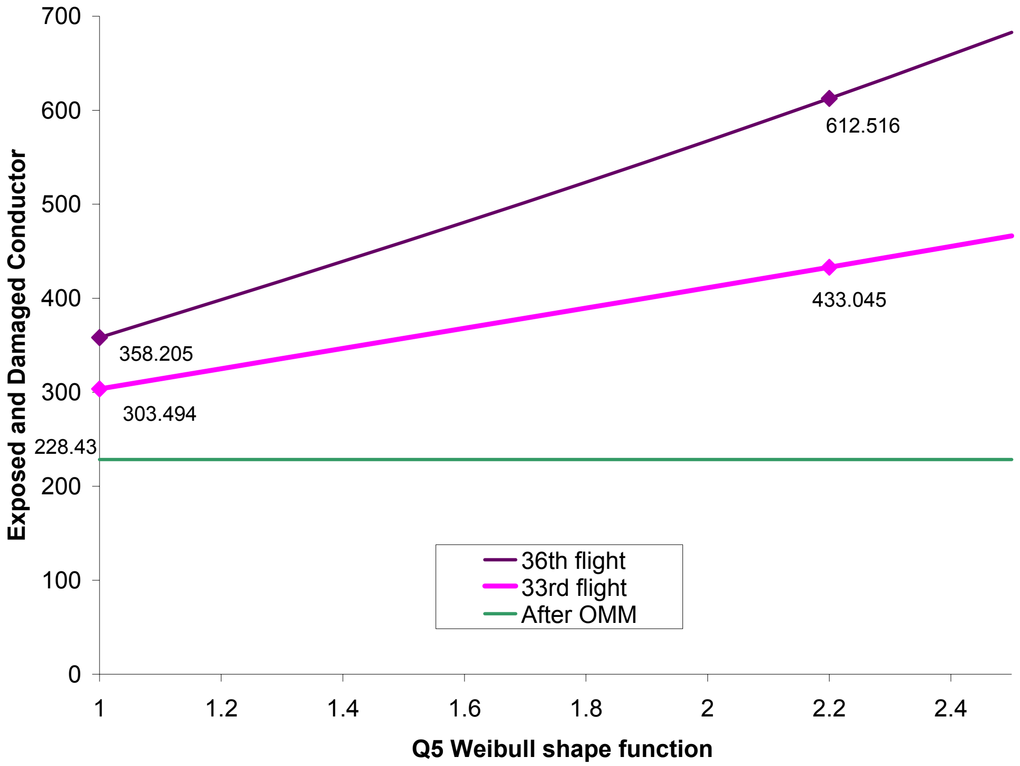


Figure C-6. Sensitivity to Weibull Shape Function: Q6=0.206

Event Description

Events 1 to 15 are described below. For the fault tree, the source of wire damage is not differentiated (as it is modeled separately), so several failure modes are grouped together. The following mapping can be identified to the FMEA list from 6.30.04:

Modes 4, 5, 6 as well as 13 and 14 correspond to WWSHORT/WWCONTACT/SMART gate;
Mode 7 to WWSHORT/WWCONTACT /INDUCED/CONTAMINATED;
Mode 8 to WWSHORT/WWCONTACT /INDUCED/CONDUCTOR; and
Mode 11 to WWSHORT/WWCONTACT/ARCING/ARC/GROUND.

1. **FIRSTDOC:** Probability that a uniformly-distributed event (such as a short) occurs for the first time during docking. P_1 is calculated as a fraction of the docking time to the total power-on time: $P = T_{docking}/(T_{inflight}+T_{ground}) = 0.090546$. Appropriate numbers are extracted from the SAIC Report: $T_{inflight} = 29722h/113 = 263.02$ and $T_{ground} = (193352-29722)/98 = 1669.7$. Please note that different numbers of flights were used to calculate ground and flight hours in the SAIC report.

2. **FARFIELD (type S):** Arc reaches a coil wire.

3. **POWERDAMAGE:** Frequency of damage in power wire in the RJD bundle to be compromised where the value is proportional to the total length of "capable" (i.e., denoted in blue on the connector 22P67 diagram)

wires. AMES used the assumption that there are 40k feet of such wires (10 times more than signal wires). Based on the connector configuration, this number can be too large (in the table, the 4k value is used instead, which might be a conservative assumption). This value is directly proportional to P_{damage}: $F_{power} = P_{damage}L_{power}\eta_{comprom}$. Here $\eta_{comprom}$ refers to the fraction of wire damage that is relevant to creating a power short (in the present calculation, $\eta_{comprom} = 1.0$). Note the value of P_{damage} used in the fault tree corresponds to the 33rd flight of OV-103 (see Figure C-3).

4. **EXPOSED:** Frequency of exposed wires for control wire in RJD bundle. This value is directly proportional to P_{damage}: $F_{control} = P_{damage}L_{control}\eta_{exposed}$. Here, η exposed refers to the fraction of wire damage that provides enough exposed conductor that leads to the short (the same as previous).

5. **CCF:** Neighboring wires are exposed (Common Cause Failure) and are in close contact. This is not improbable since two neighboring wires are likely to be exposed to a similar environment. This event is considered to be dynamic (of type D, as described above). The probability of this event per single flight is based on the following calculation where two inputs are used: P_{et} (total probability that event will happen). D_{exp} (expected delay associated with this event): $P_{event} = P_{et}\left(1-\exp\left[\frac{1}{D_{\exp}}\right]\right)$ (constant failure rate is assumed to minimize number of parameters).

6. **NEARFIELD (type S):** One of the exposed neighboring wires is power. Significantly less than 0.5 if 22P67 connector is representative. Still non-negligible since wires can change their relative positions away from connectors (and other connector can be different).

7. **WWCONTACT (type S):** Two neighboring damaged wires enter into close contact (the contact is sufficient to initiate a short).
WGCONTACT (Event 7a, type D): Compromised segment of wire contacts ground. Total probability is lowered from 0.5 to 0.05 in accordance with Glenn Williams' comments on July 5, 2004. Calculations are analogous to CCF event.

8. **SLOW1 (type S):** Initiation of wire-to-ground contact is slow enough (low current) to allow carbonization. Per discussion with Mark Hetzel, this event is less likely than Event 10 since the short with ground is more likely to be swift (i.e., high current), thus tripping the fuse before carbonization.

9. **CCF2 (type D):** Neighboring power wiring is damaged (Common Cause Failure) and in close contact. It is likely to be significantly higher than Event 5 as power wires are expected to be a twisted pair and damage of the wires, rather than exposed wire, is required (similar in the Event 8, the scale factor of 100 is used to balance Event 3).

10. **SLOW2:** Initiation of wire-to-wire contact is slow enough (low current) to allow carbonization. See Event 8, with two wires damaged, but not fully exposed, slow (low current) event is more likely.

11. **CONTAMINATION:** Contamination occurs that rapidly degrades wire integrity. Improbable.

12. **UNDETECTED:** Contamination is undetected long enough to damage wires.

13. **WWINDUCED:** Damaged wire led to a short between power and signal wire, either directly via smart short or indirectly via arcing. Can be developed further to investigate the modes similar to ARCING and SMART gates (see the fault tree). However, the impact of this event is minimal.

14. **EXTCONDUCTOR:** External conductor is introduced remote.

15. **CRACKED:** Relevant wires are compromised. Proportional to the total damage similar to Events 3 and 4; η allows for damage of both signal and power wire. However, total probability rather than frequency of occurrence is required.

Darlington Pair

The failure modes are grouped in the following broad categories: Internal Transistor, RJD Wiring, Induced Failures, Connector Failures, and Sensitivity to RJD Power-on.

Internal Transistor

Total failure rates of two transistors for a Darlington pair are taken to be $\lambda_3 = 5.0\times10^{-8}$and $\lambda_4 = 2.0\times10^{-8}$, respectively (based on AT&T Reliability Manual [22]. In the present PRA, it is assumed that approximately 60% of all failures result in a transistor short. It must be noted that 0.01% used in the SAIC report is considered to be unrealistic. In fact, one of the RAC sources indicates as much as 73% of all the transistor failures lead to shorts. There are 38 thrusters, and the total operating time is assumed to be five hours. The total probability of at least one failure during this time frame is $P_{DS} = 1 - [\exp(-5\times 0.6\times(\lambda_3 + \lambda_4))]^{38} = 7.98 \times 10^{-6}$.

This total probability is apportioned among the following five modes. This apportionment does not affect the probability of the top-level event, but identification of these modes can be important for the follow up analysis.

16. **COLEMITT (Mode 19):** Collector to emitter short of any driver or output Darlington transistor. Cited in the SAIC report where 0.1% fraction of total failures is not considered to be credible, instead 20% of total shorts are assumed.

17. **COLBASE (Mode 20):** Collector to base short of any driver or output Darlington transistor. Similarly to the previous mode cited in the SAIC report where 0.1% fraction of total failures is not considered to be credible, instead 20% of total shorts are assumed.

18. **DCONTAM (Mode 23):** The following modes from the SAIC report are identified as relevant to this group: Conductive contaminant in any driver or output; Contamination; and Contaminated (1.9% and 0.1% of total transistor failures, respectively). In the present study, 20% of total shorts are contributed to this group.

19. **DARLEAK (Mode 16):** Excessive leakage current due to aging, degraded metallization, or leaky hermetic seal in a driver Darlington transistor. Several modes relevant to this group are identified from Appendix B in the SAIC report (values shown are reported percentages of total transistor failures: Metallization 0.7%, Seal Failure 0.6%, High Leakage Current 0.6%, Leakage 0.3%, and Hermetic Leakage 0.1%). Presently, 30% of shorts are contributed to this group.

20. **INTERMETALLIC (New mode suggested by Henning Leidecker) Growth of intermettalic compounds in wire bond:** This can lead to either open or erratic resistant conditions. The SAIC report list contains the following modes: "Wire bond failure" and "Intermetallic growth" (0.7% and 0.1% of total transistor failures, respectively). Presently, 10% of shorts are assumed to contribute to the shorts of the transistor.

RJD Wiring

21. **TRANSFORMER (Mode 31):** Internal RJD box wire short of any driver or output Darlington transistor emitter, or base lead wire to 28 VDC conductor or terminal due to degradation of the insulation transformer. Currently, the probability of this failure is considered to be negligibly small.

22. **LEAKPATH (Mode 15):** Internal leakage path across circuit board or wiring (most likely scenario is Teflon's cold flow). This type of failure corresponds to "infant mortality" events, and it is expected that it would have happened already. The resulting probability is considered to be negligible.

23. **INTCONT (Mode 23):** Conductive (liquid?) contaminant between Darlington transistor case and base pin. Failure rate is assumed to be $\lambda_{23}= 1.0\times 10^{-9}$. There are 38 thrusters operating for five hours, so the total probability of at least one failure during this time frame is $P_{23} = 1 - [\exp(-5(\lambda_{23}))]^{38} = 1.9 \times 10^{-7}$.

24. **WHISKERS (Mode 23):** Another possible source of conductive contaminant between the Darlington transistor case and base pin. Failure rate is assumed to be $\lambda_{23b}=1.0 \times 10^{-9}$. The calculations that are identical to the previous item also provide the total probability 1.9×10^{-7}.

Induced Failures

25. **Mode 18 Shorted Darlington:** Output transistor caused by turn on into an intermittent output command wire short to chassis that shorts transistor but does not open 7A fuse. SLOWFUSE Measure of the short to be “intermittent enough” to damage transistor before the fuse blows, assumed to be 0.01.

26. **Mode 25 ESD (immediate and latent):** Output transistor. There is a protection, but human errors can be potentially important. More modeling is desirable. Based on total rate $1.0E^{-7}$.

27. **ENERGIZED:** For a failure Mode 18 to occur, the RJD box needs to be powered on during the short.

Connector Failures

This portion of the FT has not been developed, but corresponds to Mode 3.

Sensitivity to RJD Power-on

Figure C-7 demonstrates sensitivity of the probability of inadvertent firing due to a Darlington pair failure as a function of powered-on time of the RJD box during mating. Note that all other assumptions are kept the same and the time is varied between 0.5 and 20 hours.

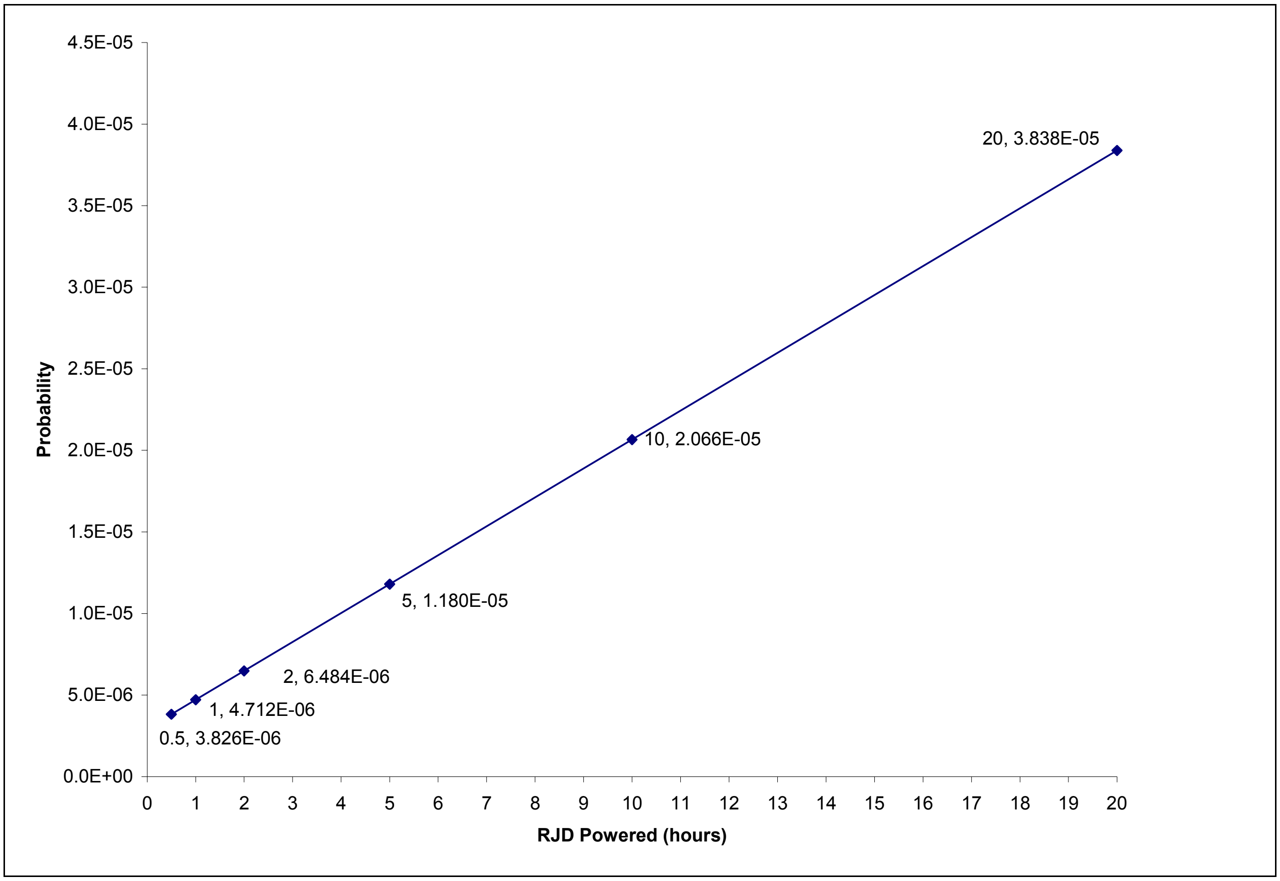


Figure C-7. Sensitivity of Darlington Pair Failure with Respect to Powered On Time During Mating

References

1. Samandar Roshan-Zamir. *"Point Estimate Analysis of the Probability of Wire-to-Wire Short in the RCS Ares"*, SAIC, Shuttle Analysis/S&MA, May 26, 2004.
2. Koushik Datta and Owen R. Greulich. *"Risk Assessment of Wire Failures Causing Uncommanded Orbiter RCS Firing While Docked at the ISS"*, National Aeronautics and Space Administration, Ames Research Center, October 29, 2003.
3. E. Henley and H. Kumamoto. *Probabilistic Risk Assessment: Reliability Engineering, Design, and Analysis, IEEE Press*, Piscataway, 1992.
4. T. Bedford and R. Cooke. *Probabilistic Risk Analysis: Foundations and Methods. Cambridge University Press*, Cambridge, 2001.
5. Michael Stamatelatos et al, "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners," Version 1.1. Office of Safety and Mission Assurance, NASA Headquarters, Washington DC, August 2002.
6. C. Perrow, Normal Accidents, Basic Books, New York, 1986.
7. D. Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*, University of Chicago Press, Chicago, 1996.
8. W.L. Oberkampf, J. C. Helton, C. A. Joslyn, S. E. Wojtkiewicz, and S. Ferson, "Challenge problems: uncertainty in system response given uncertain parameters" *Reliability Engineering and System Safety*, vol. 85, 2004, pp.11-19.
9. G. J. Klir and R. M. Smith "On measuring uncertainty and uncertainty-based information: Recent developments", *Annals of Mathematics and Artificial Intelligence*, vol. 32, 2001, pp. 5-33.
10. L. A. Zadeh, "Fuzzy Sets", *Information and Control* vol. 8 1965, pp. 338-353.
11. A. Villemeur, *Reliability, Availability, Maintainability, and Safety Assessment* Chichester, New York: J. Wiley, vol.1, 1992.
12. S. E. Rigdon and A. P. Basu. *Statistical Methods for the reliability of repairable systems*, Wiley and Sons, 2000.
13. CAIB Report, 2003.
14. D. Kahneman et al, Eds. *Judgment under Uncertainty: Heuristics and Biases* Cambridge University Press, Cambridge, 1982.
15. S. G. Vick. *Degrees of Belief. Subjective Probability and Engineering Judgment*, ASCE Press, Reston, 2002.
16. W. G. Schneeweiss, The Fault Tree Method (in the fields of reliability and safety technology), LiLoLe-Verlag, Hagen, 1999.
17. W. Vesely, F. Goldberg, N. Roberts, D. Haasl. Fault Tree Handbook, NUREG, Washington, 1981.
18. A. Bobbio, L. Portinale, M. Minichino, E. Ciancamerla, "Improving the Analysis of Dependable Systems by Mapping Fault Trees into Bayesian Networks", *Reliability Engineering and System Safety*, Vol. 71, 2001, pp. 249-260.
19. W.G. Schneeweiss, Petri Nets for Reliability Modeling, LiLoLe-Verlag, Hagen, 1999.
20. V.V. Volovoi, "Modeling of System Reliability Using Petri Nets with Aging Tokens", *Reliability Engineering and System Safety*, vol. 84, pp. 149–161, 2004.
21. Denison, D.G.T., Holmes, C.C., Mallick, B.K., and Smith, A.F.M., *Bayesian Methods for Nonlinear Classification and Regression,* Wiley, 2002.
22. D.H. Klinger, Y. Nakada, M. A. Menendez. *AT&T Reliability Manual*, Van Nostrand Reinhold Company ISBN 0-442-31848-0, 1990, Table 4.6, page 141.

Table C-1. Input Parameters to Wire Damage Evolution Model

Confidence levels: 🟩 HIGH 🟨 MEDIUM 🟥 LOW

Par	Name	Description	Value (P)	Justification	Source/Comparison
🟨 1	INITIAL	Fraction of damaged wires that were damaged from the very beginning	0.15	It is assumed that 15% of the damage detected during OMDP are due to initial installation	
🟨 2	DETECTBEFORE	Fraction of detected (and repaired) damage per turn-around before 1999 (includes OMDP)	0.04	Note that average SD per flight recorded in PRACA prior to 1999 is about 17 SD, model should be consistent with PRACA data	
🟨 3	DETECTMAJOR	Fraction of detected damage during the last OMDP	0.7		
🟨 4	DETECTAFTER	Fraction of detected damage per turn-around after 1999	0.1	Previously assumed 0.2 is too high, based on the data for 0V-103 (unless other parameters from this model are changed)	NASA Ames report assumes that the ratio between P4 and P2 is 1: 6 (but therein effects of MAINTIMPROVE are rolled in as well)
🟨 5	WEIBULL	Weibull shape parameter associated with the damage that is not maintenance induced.	1 (2.2)	Initially constant failure rate was considered (value 1). Data in Appendix G suggests value as high as 2.2 (see Figures C-4 and C-5).	
🟨 6	MAINTCAUSE	Fraction of new damaged that was induced by maintenance (before 1999)	0.9 (0.206)	It was initially assumed that 90% of damage is induced leading to 0.9 value. However, in accordance with Appendix G, the induced damage constitutes about 0.175 of the total damage, which leads to the value of Q6 as low as 0.206	
🟥 7	MAINTIMPROVE	Fraction of maintenance induced damage after 99 as compared to pre- 99 procedures	0.1	10 times improvement is assumed	Ames report cites P6 to P7 as 100: 1

Table C-2. Basic Events For Wire-To-Wire Fault Tree

Type: S- static (no delay); D- dynamic (delay specified) INPUT

Total amount of significant damage 204.3

Event	Name	Type	Description	Delay (flights)	total P	η	wire length (ft)	Value for FTA	Justification
1	FIRSTDOC	S	Short occurs for the first time during docking	0				0.09055	Fraction of powered operation during docking. Exposure is consistent with SAIC report.
2	FARFIELD	S	Arc reaches a coil wire	0				0.6	Even near connector the wires are separated only by two wires.
3	POWERDAMAGE	S	Frequency of power wire compromised in RJD bundle	0		1	4000	4.25666	22P67 RJD bundle has half as many power wires as coil wires (i.e. 2000 feet), here 4000 is used; amount of significant damage is from wire damage evolution model; Fraction of relevant damage is given as 1 (damaged and exposed conductor).
4	EXPOSED	S	Frequency of coil wire exposed	0		1	4000	4.25666	4k of wires, fraction of relevant damage is 1 (the same as above).
5	CCF	D	Neighboring wire is exposed (Common Cause Failure)	5	0.1			0.01813	This is not improbable, as two neighboring wires are likely to be exposed to similar environment.
6	NEARFIELD	S	One of the exposed neighboring wire happens to be power	0				0.2	Non-negligible, even if 22P67 connector is representative, as wires can change their relative positions away from connectors. NASA Ames report used a generic value 0.1.
7	WWCONTACT	S	Two damaged wires come in close contact					0.05	Can be considered to be dynamic.
7a	WGCONTACT	D	Compromised segment of power wire contacts ground	6	0.03			0.00461	
8	SLOW1	S	Initiation of wire-to-ground contact is slow enough (low current) to allow carbonization	0				0.005	This event is less likely than event 10 as the short with ground is more likely to be swift (i.e. high current), thus tripping the fuse before carbonization.

Table C-2. Basic Events For Wire-To-Wire Fault Tree

Type: S- static (no delay); D- dynamic (delay specified) INPUT

Total amount of significant damage 204.3

Event	Name	Type	Description	Delay (flights)	total P	η	wire length (ft)	Value for FTA	Justification
9	CCF2	D	Given damaged power wire, a neighboring return wire is damaged (Common Cause Failure) and the two are in close contact	5	0.2			0.03625	Likely to be significantly higher than Event 5 as power wires are expected to be a twisted pair that is more prone to tracking.
10	SLOW2	S	Initiation of wire-to-wire (power to return) contact is slow enough (low current) to allow carbonization	0				0.2	See Event 8, with two wires damaged, but not fully exposed, slow (low current) event is more likely.
11	CONTAMINATION	S	Contamination occurs that rapidly degrades wire integrity	0				1.0E-04	Corresponds to "remote" probability
12	UNDETECTED	S	Contamination is undetected long enough to damage wires	0				0.001	
13	WWINDUCED	D	Damaged wire led to a short between power and signal wire (either directly via smart short or indirectly via arcing)					0.2	Modes are similar to ARCING and SMART gates (see the fault tree) except occurring in an accelerated fashion estimated here as 0.2 is not developed further due to low probability of Events 11 and 12.
14	EXTCONDUCTOR	S	External conductor is introduced					1.0E-03	Can be conductive liquid media or debris (like event 11 is considered to be a remote probability)
15	CRACKED	D	Relevant wires are compromised			0.05	4000	0.19171	Proportional to the total damage; allows for damage of both coil and power wire; total probability rather than frequency of occurrence is required.

Table C-3. Basic events for Darlington Pair Fault Tree

Event	Name	Description	Value (P)	Justification
16	COLEMITT	Collector to emitter short of any driver or output Darlington transistor, Mode 4	1.596 E^{-6}	Events 16-20 based on two units 5 10-8 and 2.0 10-8 and 60% is of transistor shorts. This leads to the total probability of failure due to Darlington pairs Pds=7.98 E^{-6} (for 38 thrusters for 5 hours of operation, see main text. The event contributes 20%
17	COLBASE	Collector to base short of any driver or output Darlington transistor, Mode 5	1.596 E^{-6}	Event 17 is 0.2 Pds (see Event 16)
18	DCONTAM	Conductive contaminant in any driver or output Darlington transistor, Mode 6	1.596 E^{-6}	Event 18 is 0.2 Pds (see Event 16)
19	DARLEAK	Excessive leakage current due to aging, degraded metallization, or leaky hermetic seal in a driver Darlington transistor; Mode 7, 27	2.394 E^{-6}	Event 19 is 0.3 Pds (see Event 16)
20	INTERMETALLIC	Growth of intermetallic compounds wire bond (New mode, HL)	7.98 E^{-7}	Event 20 is 0.1 Pds (see Event 16)
21	TRANSFORMER	Degradation of the isolation transformer Mode 9, 24b	0	Lower than transistor unless 150 degrees is 1-2 10-9 or high voltage subject Spice analysis irrelevant.
22	LEAKPATH	Internal leakage path across circuit board or wiring Modes 9, 24a, 31	0	No multi-layer circuit board, only wire can pinched, highly unlikely, cold Teflon flow given that it did not happen (needs to be checked against PRACA).
23	INTCONT	Conductive (liquid?) contaminant between or debris case and base pin Modes 10, 26	1.9 E^{-7}	Debris like a single screw filing. The number is based on a failure rate 1E^{-9} per hour for a single thruster
24	WHISKERS	Another source of conductive contaminant 10,26	1.9 E^{-7}	Conformally coated, the odds are that we do not have tin whiskers. The number is based on a failure rate 1E^{-9} per hour for a single thruster
25	SLOWFUSE	Transistor fails before the fuse blows	0.01	Measure of the short to be "intermittent enough" to damage transistor before the fuse blows.
26	ESD	Transistor failure induced by ESD	5.0 E^{-7}	Output transistor. There is a protection but human errors can be potentially important. More modeling is desirable. Based on total rate (not for individual transistor of 1.0E^{-7}).
27	ENERGIZED	RJD box is energized	0.3	

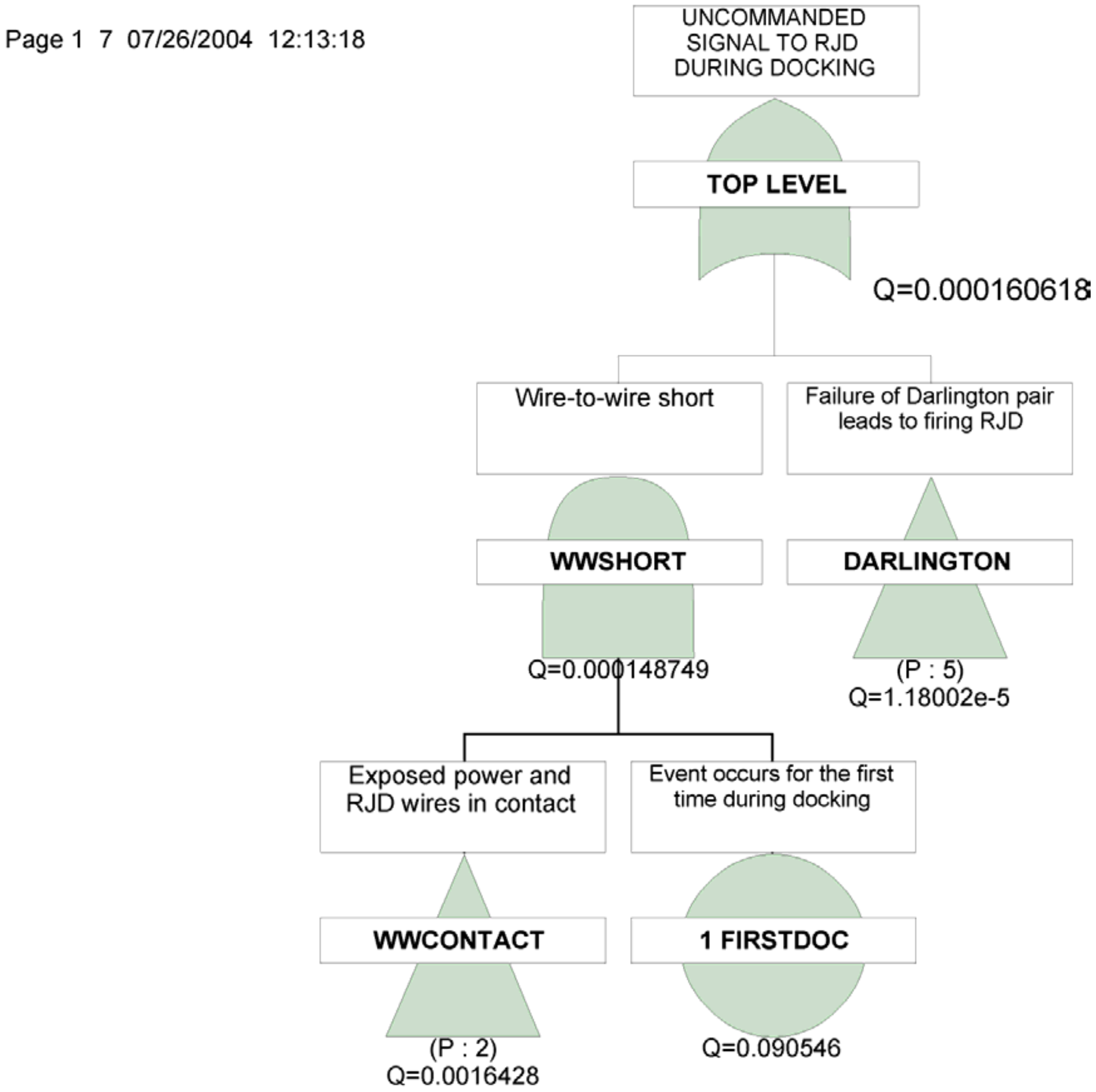
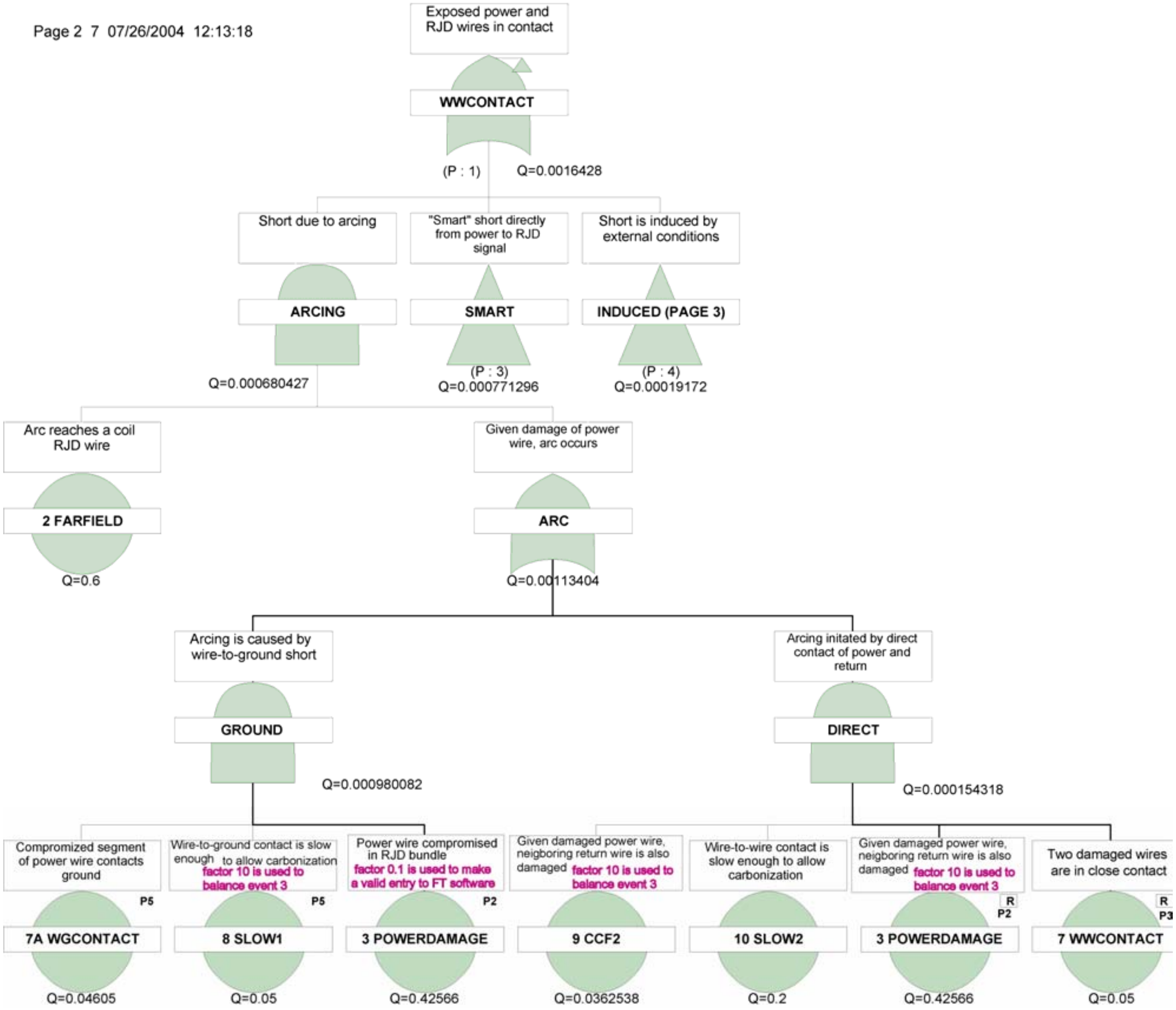

Page 1 7 07/26/2004 12:13:18
UNCOMMANDED SIGNAL TO RJD DURING DOCKING
TOP LEVEL
Q=0.000160618
Wire-to-wire short
Failure of Darlington pair leads to firing RJD
WWSHORT
DARLINGTON
Q=0.000148749
(P : 5)
Q=1.18002e-5
Exposed power and RJD wires in contact
Event occurs for the first time during docking
WWCONTACT
1 FIRSTDOC
(P : 2)
Q=0.0016428
Q=0.090546

Figure C-8. Fault Tree (page 1 of 7)



Page 2 7 07/26/2004 12:13:18
Exposed power and RJD wires in contact
WWCONTACT
(P : 1)
Q=0.0016428
Short due to arcing
ARCING
Q=0.000680427
"Smart" short directly from power to RJD signal
SMART
(P : 3)
Q=0.000771296
Short is induced by external conditions
INDUCED (PAGE 3)
(P : 4)
Q=0.00019172
Arc reaches a coil RJD wire
2 FARFIELD
Q=0.6
Given damage of power wire, arc occurs
ARC
Q=0.00113404
Arcing is caused by wire-to-ground short
GROUND
Q=0.000980082
Arcing initated by direct contact of power and return
DIRECT
Q=0.000154318
Compromized segment of power wire contacts ground
P5
7A WGCONTACT
Q=0.04605
Wire-to-ground contact is slow enough to allow carbonization
factor 10 is used to balance event 3
P5
8 SLOW1
Q=0.05
Power wire compromised in RJD bundle
factor 0.1 is used to make a valid entry to FT software
P2
3 POWERDAMAGE
Q=0.42566
Given damaged power wire, neigboring return wire is also damaged
factor 10 is used to balance event 3
9 CCF2
Q=0.0362538
Wire-to-wire contact is slow enough to allow carbonization
10 SLOW2
Q=0.2
Given damaged power wire, neigboring return wire is also damaged
factor 10 is used to balance event 3
R
P2
3 POWERDAMAGE
Q=0.42566
Two damaged wires are in close contact
R
P3
7 WWCONTACT
Q=0.05

Figure C-9. Fault Tree (page 2 of 7)

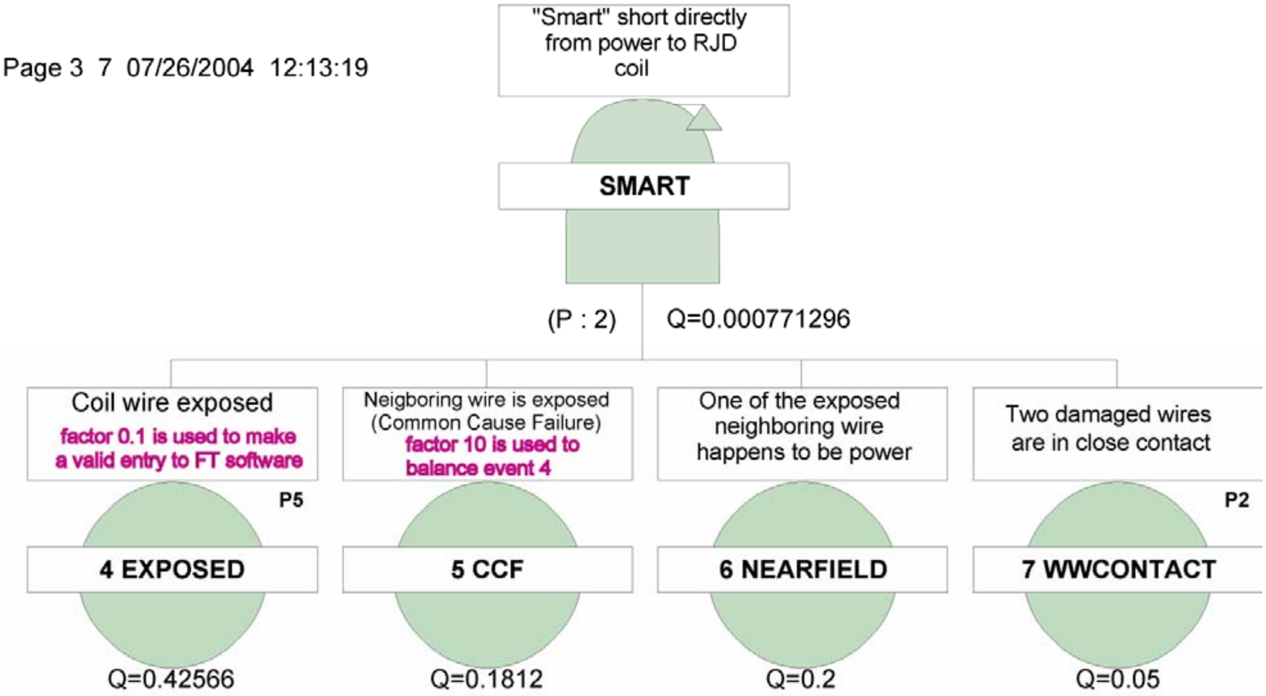

Page 3 7 07/26/2004 12:13:19
"Smart" short directly from power to RJD coil
SMART
(P : 2)
Q=0.000771296
Coil wire exposed
factor 0.1 is used to make a valid entry to FT software
P5
4 EXPOSED
Q=0.42566
Neigboring wire is exposed (Common Cause Failure)
factor 10 is used to balance event 4
5 CCF
Q=0.1812
One of the exposed neighboring wire happens to be power
6 NEARFIELD
Q=0.2
Two damaged wires are in close contact
P2
7 WWCONTACT
Q=0.05

Figure C-10. Fault Tree (page 3 of 7)

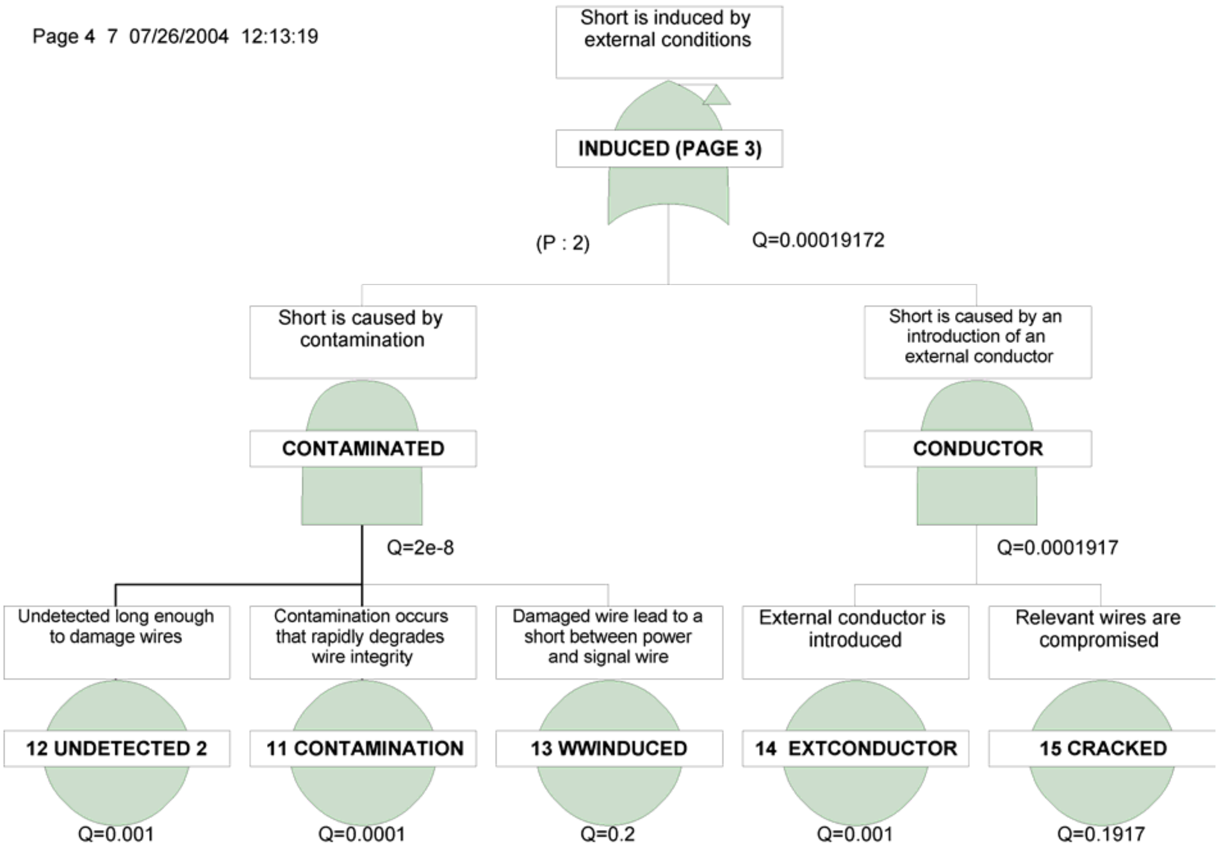

Page 4 7 07/26/2004 12:13:19
Short is induced by external conditions
INDUCED (PAGE 3)
(P : 2)
Q=0.00019172
Short is caused by contamination
CONTAMINATED
Q=2e-8
Short is caused by an introduction of an external conductor
CONDUCTOR
Q=0.0001917
Undetected long enough to damage wires
12 UNDETECTED 2
Q=0.001
Contamination occurs that rapidly degrades wire integrity
11 CONTAMINATION
Q=0.0001
Damaged wire lead to a short between power and signal wire
13 WWINDUCED
Q=0.2
External conductor is introduced
14 EXTCONDUCTOR
Q=0.001
Relevant wires are compromised
15 CRACKED
Q=0.1917

Figure C-11. Fault Tree (page 4 of 7)

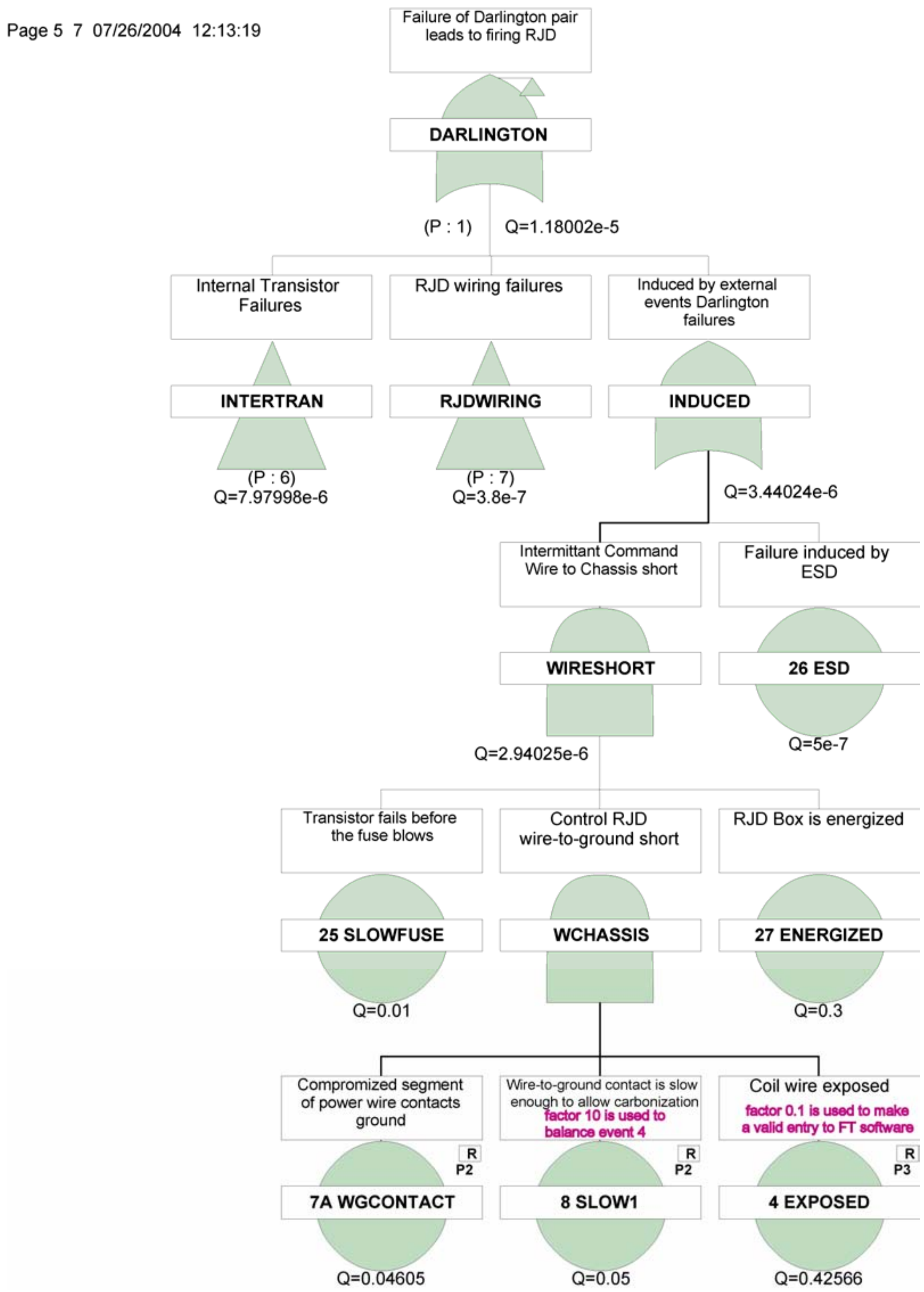

Page 5 7 07/26/2004 12:13:19
Failure of Darlington pair leads to firing RJD
DARLINGTON
(P : 1)
Q=1.18002e-5
Internal Transistor Failures
INTERTRAN
(P : 6)
Q=7.97998e-6
RJD wiring failures
RJDWIRING
(P : 7)
Q=3.8e-7
Induced by external events Darlington failures
INDUCED
Q=3.44024e-6
Intermittant Command Wire to Chassis short
WIRESHORT
Q=2.94025e-6
Failure induced by ESD
26 ESD
Q=5e-7
Transistor fails before the fuse blows
25 SLOWFUSE
Q=0.01
Control RJD wire-to-ground short
WCHASSIS
RJD Box is energized
27 ENERGIZED
Q=0.3
Compromized segment of power wire contacts ground
R
P2
7A WGCONTACT
Q=0.04605
Wire-to-ground contact is slow enough to allow carbonization
factor 10 is used to balance event 4
R
P2
8 SLOW1
Q=0.05
Coil wire exposed
factor 0.1 is used to make a valid entry to FT software
R
P3
4 EXPOSED
Q=0.42566

Figure C-12. Fault Tree (page 5 of 7)

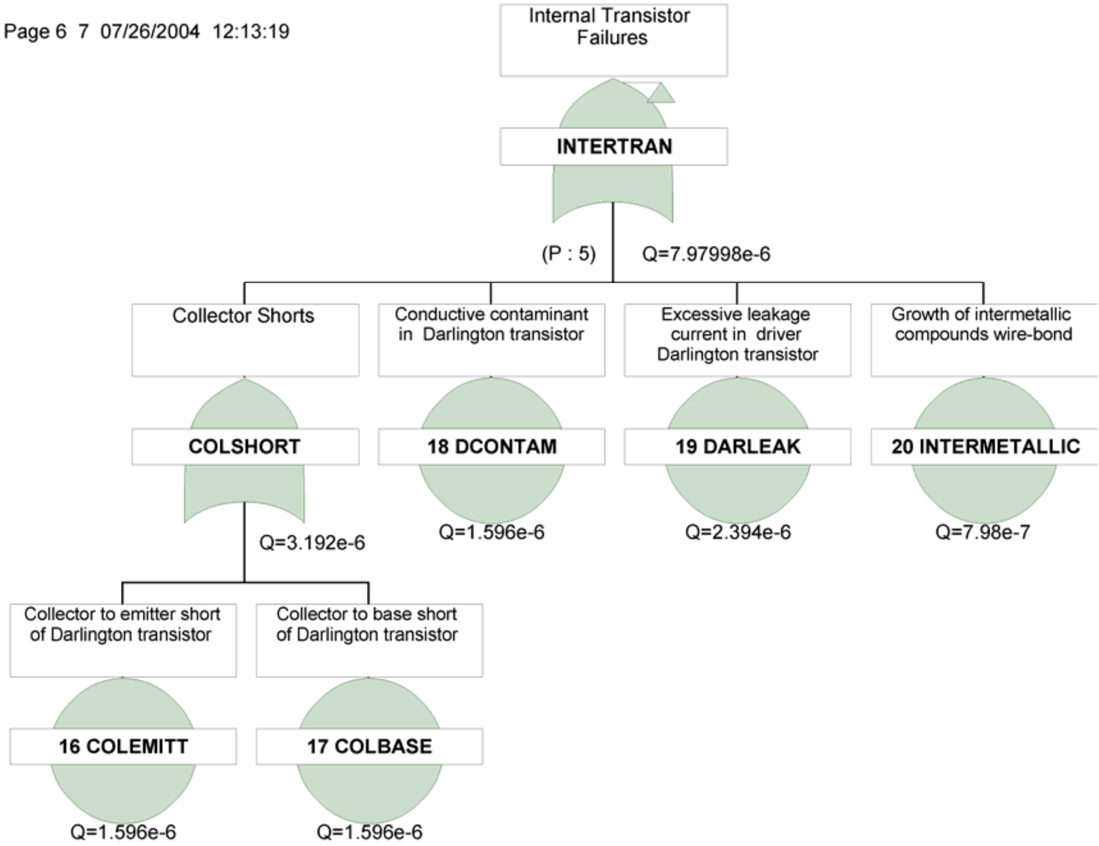

Page 6 7 07/26/2004 12:13:19
Internal Transistor Failures
INTERTRAN
(P : 5)
Q=7.97998e-6
Collector Shorts
COLSHORT
Q=3.192e-6
Conductive contaminant in Darlington transistor
18 DCONTAM
Q=1.596e-6
Excessive leakage current in driver Darlington transistor
19 DARLEAK
Q=2.394e-6
Growth of intermetallic compounds wire-bond
20 INTERMETALLIC
Q=7.98e-7
Collector to emitter short of Darlington transistor
16 COLEMITT
Q=1.596e-6
Collector to base short of Darlington transistor
17 COLBASE
Q=1.596e-6

Figure C-13. Fault Tree (page 6 of 7)

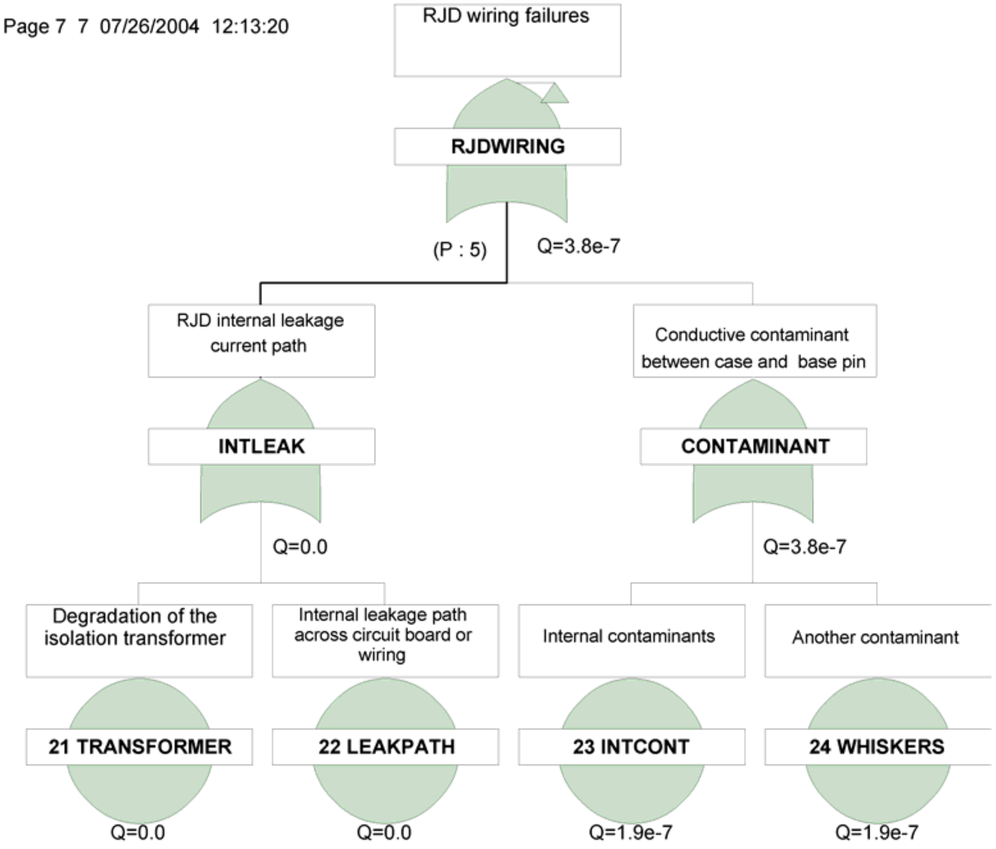

Page 7 7 07/26/2004 12:13:20
RJD wiring failures
RJDWIRING
(P : 5)
Q=3.8e-7
RJD internal leakage current path
INTLEAK
Q=0.0
Conductive contaminant between case and base pin
CONTAMINANT
Q=3.8e-7
Degradation of the isolation transformer
21 TRANSFORMER
Q=0.0
Internal leakage path across circuit board or wiring
22 LEAKPATH
Q=0.0
Internal contaminants
23 INTCONT
Q=1.9e-7
Another contaminant
24 WHISKERS
Q=1.9e-7

Figure C-14. Fault Tree (page 7 of 7)

Appendix D
Darlington Transistor Test Plan

Statement of Work for Hi-Rel Laboratories, Inc., to Test Space Shuttle Darlington Pair Transistors for the NASA Engineering and Safety Center (NESC) Reaction Jet Driver Independent Technical Assessment

Rick Gilbrech, NESC Deputy Director (757-864-2400)
3/21/05 (revision K)

Background

The Space Shuttle Program (SSP) has a zero fault tolerant design related to an inadvertent firing of the primary reaction control jets on the Orbiter during mated operations with the International Space Station (ISS). There are 44 thrusters on each Orbiter, 38 primary thruster (870 lbf thrust each) and 6 vernier thrusters (24 lbf thrust each). Failure modes which result in a failed-on primary thruster during mated operations with ISS drive forces that exceed the structural capabilities of the docked Shuttle/ISS structure. This catastrophic scenario has been an accepted risk by both programs in the past based on the probability estimates of this event occurring being remote (10^{-3} to 10^{-6} per operational opportunity) to improbable ($<10^{-6}$). NESC was asked by NASA's Chief Safety and Mission Assurance Officer to review the issue and render a technical opinion on the probability of a catastrophic failure related to this scenario. One root cause of an inadvertent primary thruster firing is failure (fail short) of the reaction jet driver (RJD) Darlington pair switch. This test program will address aging or manufacturing defects in a sample set of SSP flight transistor assets.

Statement of Work

The scope of the effort for Hi-Rel is to conduct a series of tests identified below on Darlington pair transistors (JANTXV2N5038 and JANTXV2N5665) to be supplied by the NESC. These will include fifty (50) non-flight pathfinder pairs, two (2) SSP flight spare pairs and two (2) SSP flown pairs. This test plan will be jointly reviewed and approved by NESC, the SSP liaison and Hi-Rel. The fifty (50) non-flight transistor pairs will be screened and the four (4) best performing pairs will be used as pathfinders to validate the test fixtures and procedures. Matching of pathfinder transistors shall be performed by individually screening each transistor at 100 °C to find the four best performers (lowest I_{CEO} @ 32 V_{CE}) of each type. The best four performing transistors of each type (JANTXV2N5038 and JANTXV2N5665) will be randomly paired as the pathfinder sets. These shall be marked for traceability per Steps 1b through 1d below and then put through the full testing identified in Steps 2a through 2i. Successful review and approval of the pathfinder data by the NESC and SSP liaisons will be required prior to proceeding with tests of the flight spare/flown transistors. The flight spare/flown transistor will be marked for traceability per Steps 1b through 1d and then put through the full testing identified in Steps 3a through 3i. Finally, the remaining 92 transistors will characterized at higher V_{CE} in Steps 4a through 4b.

NESC and the SSP liaison will reserve the right to inspect the facilities at Hi-Rel to be used and witness the tests (both pathfinder and flight articles) with at least a two-week notice prior to testing. ***Any deviations from this test plan must be reviewed and approved by the NESC and the Space Shuttle Program via Rick Gilbrech.***

General Requirements:

- All material shall be handled in accordance with NASA-STD-9739.7, Electrostatic Discharge (ESD) control, methods and procedures.
- A log of all steps and data shall be maintained with the initials of the person(s) conducting the test recorded for each step performed. All data shall be entered into this log along with the unique identification for the transistor being tested.
- Photographic and video records of the testing shall be maintained.
- All testing shall be conducted in the presence of NASA representatives.
- When being conducted, Destructive Physical Analysis (DPA) shall be performed on each part per MIL-STD-1580B.

1) Initial Materials Inspection

Inspect material per MIL-STD-1580B for the following:

a) Transistor pairs should be bagged in appropriate ESD control material. The bag should be free from tears and punctures and sealed. Each bag should contain the “matched” Darlington transistor pair comprising:

   i) Two individual transistors, each individually bagged – a 2N5665 and a 2N5038.

   ii) A separate ESD control bag containing identifying paperwork.

b) Ensure that each transistor received has been marked with unique identification. Paper labels with adhesives backing shall not be used.

c) Ensure that a “matched” Darlington transistor pair can be positively associated with one another.

d) Ensure that a “matched” Darlington transistor pair can be associated as originating from NESC pathfinder stock, Space Shuttle Program flight spare stock or removed from a flown RJD.

2) NESC Pathfinder Darlington Transistor Testing, Four (4) Best-Performing Pairs

The tests described in this section shall be performed on the pathfinder Darlingtons formed by the random pairing of the four transistors of each type having lowest ICEO @ 32 V_{CE}. The performance of additional electrical tests, noted herein, shall be conducted in addition to the DPA. The sequencing of tests will be performed in the order listed.

For all burn-in and active tests, power shall be applied by slowly increasing the power supply voltage from zero to the target value.

a) Perform electrical tests on individual parts at -55 °C, +25 °C and +125 °C, utilizing a curve tracer. Capture curve tracer plots via electronic image capture or photographic means for all parts. Ensure that temperatures have stabilized before recording the data and that the plots have sufficient magnification to enable the values for leakage current to be resolved. When performing these tests, V_{CE} shall be limited to 32 Vdc. All operational parameters shall be restricted as necessary to limit power dissipation and to stay within the operating limits specified in MIL-S-19500/439 (for the 2N5038) or MIL-S-19500/455A (for the 2N5665).

b) Review data to look for evidence of transistor aging or damage by comparing parts removed from RJD flight units versus those from flight spare and pathfinder stock. If no evidence of damage can be discerned from the data, and if the NASA representatives concur, proceed with further testing.

c) Establish original Darlington pairing and perform power-ON burn-in with pairs configured per equivalent RJD circuit (Figure 1) for 96 hours at 100 °C. Confirm that the Darlington output is switching by monitoring the voltage across the 11 Ω load resistor with an oscilloscope.

d) Separate parts and re-perform electrical tests at -55 °C, +25 °C and 125 °C. Capture curve tracer plots via electronic image capture or photographic means for all parts.

e) Repeat step b).

f) Re-establish the original Darlington pairing and perform the tests in Table 1 of Honeywell drawing 34024047 (Figure 4).

g) Perform MIL-STD–1580 non-destructive tests on each part (fine and gross hermeticity, particle induced noise detection (PIND) and radiographic).

h) Perform PIND tests on individual transistors using the methods specified in MIL-STD-750D (Notice 3, or later), Method 2052.2, Test Condition A. In addition to the acoustic detection described in the method, monitor for electrical conduction using the circuits depicted in Figure 2 and Figure 3. Capture evidence of transistor conduction by monitoring the voltage across the 1 kΩ load resistor using a digital storage oscilloscope. Should they occur, record representative instances of conduction via electronic image capture or photograph.

i) Continue with destructive DPA tests per MIL-STD–1580 (residual gas analysis (RGA), internal visual, scanning electron microscope (SEM), bond pull, die shear). RGA shall be conducted on the four pathfinders. Record observations photographically, as appropriate.

3) Space Shuttle Program Flight and Flight Spare Darlington Transistor Testing

The tests described in this section shall be performed on the flight and flight-spare Darlington transistor pairs. The performance of additional electrical tests, noted herein, shall be conducted in addition to the DPA. The sequencing of tests will be performed in the order listed.

For all burn-in and active tests, power shall be applied by slowly increasing the power supply voltage from zero to the target value.

a) Perform electrical tests on individual parts at -55 °C, +25 °C and +125 °C, utilizing a curve tracer. These will include base to emitter junction forward and reverse bias characterization, base to collector junction forward and reverse bias characterization and gain family of curves with V_{CE} limited to 32 Vdc. Additional tests will include collector to emitter leakage current at both 20 and 32 Vdc. Capture curve tracer plots via electronic image capture or photographic means for all parts. Ensure that temperatures have stabilized before recording the data and that the plots have sufficient magnification to enable the values for leakage current to be resolved. All operational parameters shall be restricted as necessary to limit power dissipation and to stay within the operating limits specified in MIL-S-19500/439 (for the 2N5038) or MIL-S-19500/455A (for the 2N5665).

b) Review data to look for evidence of transistor aging or damage by comparing parts removed from RJD flight units versus those from flight spare and pathfinder stock. If no evidence of damage can be discerned from the data, and if the NASA representatives concur, proceed with further testing.

c) Establish original Darlington pairing and perform power-ON burn-in with pairs configured per equivalent RJD circuit (Figure 1) for 96 hours at 100 °C. Confirm that the

Darlington output is switching by monitoring the voltage across the 11 Ω load resistor with an oscilloscope.

d) Separate parts and re-perform electrical tests of Step 3a at -55 °C, +25 °C and 125 °C. Capture curve tracer plots via electronic image capture or photographic means for all parts.

e) Repeat step 3b).

f) Re-establish the original Darlington pairing and perform the tests in Table 1 of Honeywell drawing 34024047 (Figure 4).

g) Perform MIL-STD–1580 non-destructive tests on each part (fine and gross hermeticity, particle induced noise detection (PIND) and radiographic)

h) Perform PIND tests on individual transistors using the methods specified in MIL-STD-750D (Notice 3, or later), Method 2052.2, Test Condition A. In addition to the acoustic detection described in the method, monitor for electrical conduction using the circuits depicted in Figure 2 and Figure 3. Capture evidence of transistor conduction by monitoring the voltage across the 1 kΩ load resistor using a digital storage oscilloscope. Should they occur, record representative instances of conduction via electronic image capture or photograph.

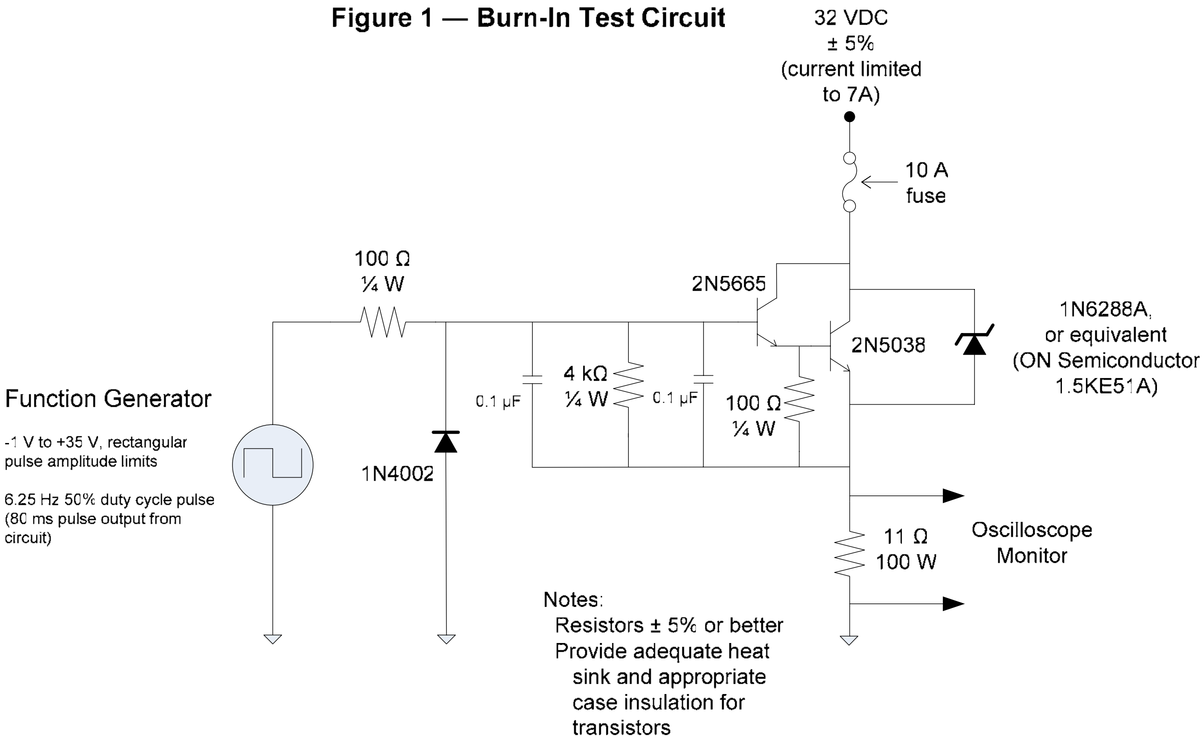
i) Continue with destructive DPA tests per MIL-STD–1580 (residual gas analysis (RGA), internal visual, scanning electron microscope (SEM), bond pull, die shear). RGA shall be conducted on only two of the four flight spare/flown Darlington pairs, to be identified by the NASA representatives. Record observations photographically, as appropriate.

4) NESC Pathfinder Transistor Testing, Remaining 92 Transistors

a) Perform electrical tests on the remaining forty-six (46) 2N5038 transistors at -55 °C, +25 °C and +125 °C, utilizing a curve tracer. Capture curve tracer plots via electronic image capture or photographic means for all parts. Ensure that temperatures have stabilized before recording the data and that the plots have sufficient magnification to enable the values for leakage current to be resolved. When performing these tests, V_{CE} shall be limited to 100 Vdc. Operational parameters shall be restricted as necessary to stay within the operating limits specified in MIL-S-19500/439.

b) Perform electrical tests on the remaining forty-six (46) 2N5665 transistors at -55 °C, +25 °C and +125 °C, utilizing a curve tracer. Capture curve tracer plots via electronic image capture or photographic means for all parts. Ensure that temperatures have stabilized before recording the data and that the plots have sufficient magnification to enable the values for leakage current to be resolved. When performing these tests, V_{CE} shall be limited to 300 Vdc. Operational parameters shall be restricted as necessary to stay within the operating limits specified in MIL-S-19500/455A.

Figure 1 — Burn-In Test Circuit



Notes:
Resistors ± 5% or better
Provide adequate heat sink and appropriate case insulation for transistors

Figure 2 — PIND Test Circuit (2N5665)

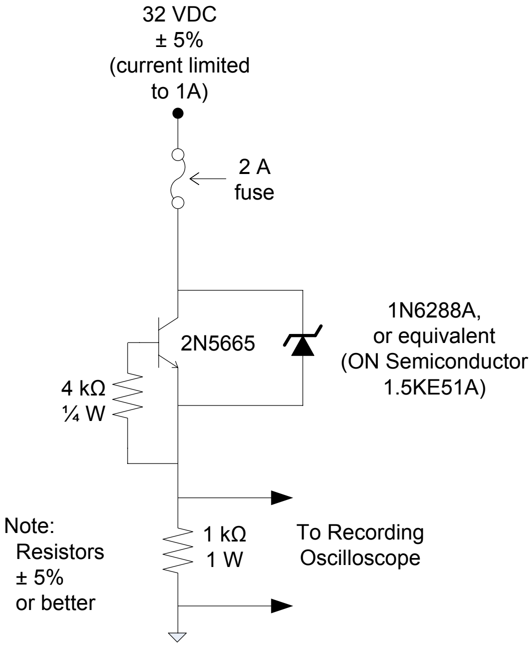
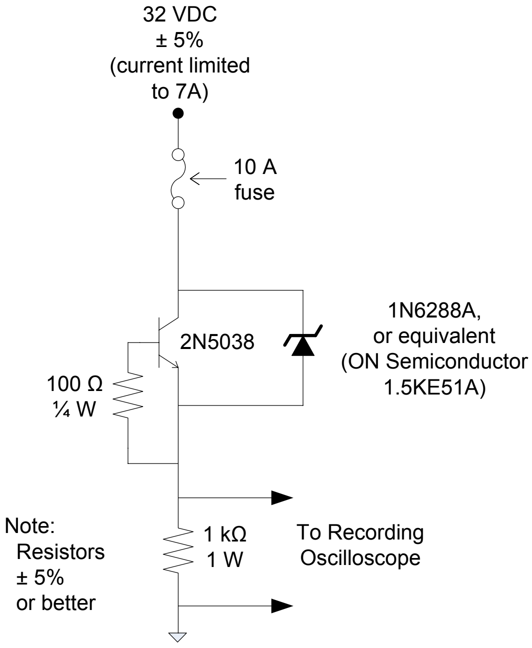
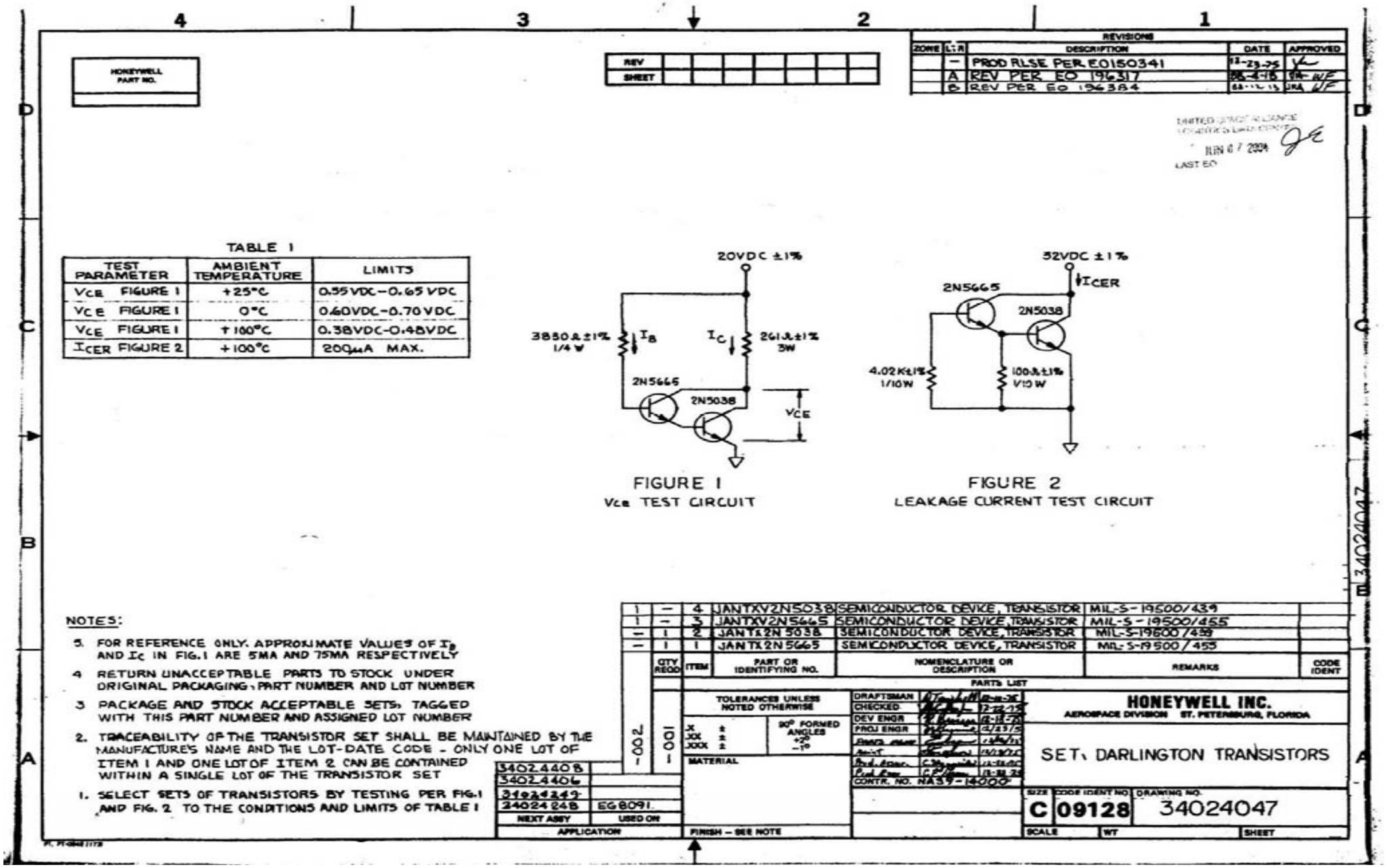


Figure 3 — PIND Test Circuit (2N5038)





REVISIONS

ZONE	LTR	DESCRIPTION	DATE	APPROVED
	—	PROD RLSE PER EO150341	12-23-75	
	A	REV PER EO 196317	86-4-16	WF
	B	REV PER EO 196384	88-12-13	WF

UNITED SPACE ALLIANCE
LOGISTICS DATA CENTER
JUN 0 7 2004
LAST EO

TABLE 1

TEST PARAMETER	AMBIENT TEMPERATURE	LIMITS
V_{CE} FIGURE 1	+25°C	0.55VDC–0.65VDC
V_{CE} FIGURE 1	0°C	0.60VDC–0.70VDC
V_{CE} FIGURE 1	+100°C	0.38VDC–0.48VDC
I_{CER} FIGURE 2	+100°C	200μA MAX.

FIGURE 1
V_{CE} TEST CIRCUIT

FIGURE 2
LEAKAGE CURRENT TEST CIRCUIT

NOTES:

5. FOR REFERENCE ONLY. APPROXIMATE VALUES OF I_B AND I_C IN FIG. 1 ARE 5MA AND 75MA RESPECTIVELY
4 RETURN UNACCEPTABLE PARTS TO STOCK UNDER ORIGINAL PACKAGING, PART NUMBER AND LOT NUMBER
3 PACKAGE AND STOCK ACCEPTABLE SETS, TAGGED WITH THIS PART NUMBER AND ASSIGNED LOT NUMBER
2. TRACEABILITY OF THE TRANSISTOR SET SHALL BE MAINTAINED BY THE MANUFACTURE'S NAME AND THE LOT-DATE CODE - ONLY ONE LOT OF ITEM 1 AND ONE LOT OF ITEM 2 CAN BE CONTAINED WITHIN A SINGLE LOT OF THE TRANSISTOR SET
1. SELECT SETS OF TRANSISTORS BY TESTING PER FIG. 1 AND FIG. 2 TO THE CONDITIONS AND LIMITS OF TABLE 1

NEXT ASSY	USED ON
34024408	
34024406	
~~34024249~~	
24024248	EG8091.

APPLICATION

PARTS LIST

-002	-001	ITEM	PART OR IDENTIFYING NO.	NOMENCLATURE OR DESCRIPTION	REMARKS	CODE IDENT
1	—	4	JANTXV2N5038	SEMICONDUCTOR DEVICE, TRANSISTOR	MIL-S-19500/439	
1	—	3	JANTXV2N5665	SEMICONDUCTOR DEVICE, TRANSISTOR	MIL-S-19500/455	
—	1	2	JANTX2N5038	SEMICONDUCTOR DEVICE, TRANSISTOR	MIL-S-19500/439	
—	1	1	JANTX2N5665	SEMICONDUCTOR DEVICE, TRANSISTOR	MIL-S-19500/455	

QTY REQD

TOLERANCES UNLESS NOTED OTHERWISE
.X ±
.XX ±
.XXX ±
90° FORMED ANGLES +2° −1°
MATERIAL
FINISH — SEE NOTE

DRAFTSMAN	[illegible]	12-10-75
CHECKED	[illegible]	12-22-75
DEV ENGR	[illegible]	12-18-75
PROJ ENGR	[illegible]	12/23/75
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
Prod. Assur.	C. [illegible]	12-22-75
Prod. Engr.	C.P. [illegible]	12-22-75
CONTR. NO.	NAS9-14000	

HONEYWELL INC.
AEROSPACE DIVISION ST. PETERSBURG, FLORIDA

SET, DARLINGTON TRANSISTORS

SIZE	CODE IDENT NO.	DRAWING NO.
C	09128	34024047

SCALE | WT | SHEET

Figure 4. Honeywell Drawing 34024047

Appendix E

RJD Shielded Wire Dry Arc-Track Test

Rick Gilbrech, NESC
757-864-2400
February 11, 2005

Objective of Test

To determine which Reaction Jet Driver valve-coil wire harness configuration has better resistance against arc-tracking. Options are: 1) unshielded wire, no over wrap (baseline Orbiter); 2) shielded wire, no over wrap; 3) shielded wire with protective over wrap; and 4) unshielded wire with protective over wrap. The protective over wrap will be PTFE wrap, Mystik 7503 tape or Teflon convoluted tubing (#MB0150-081). All wiring samples and protective over wrap materials will be supplied by the NESC.

Wire Needed

- 300-ft. of twisted-pair 20AWG polyimide replacement Orbiter wire per MB0150-048
- 200-ft. of twisted-pair shielded and jacketed 20 AWG polyimide replacement Orbiter wire
- 100-ft. of twisted-quad 20AWG polyimide replacement Orbiter wire per MB0150-048

NOTE: **Fabrication of harnesses will be done by Lectromec following the Space Shuttle Program wiring specs ML030-0014 rev. N and ML030-0013 rev. D provided by the NESC.**

Harness No. 1 Configuration

See Figure E-2. The 30VDC power and return wires are twisted-pair 20AWG wires, approximately 16 inches long. The Fuel and Ox wires are a twisted quad, unshielded. The 30VDC wires are fused to sustain maximum arc track length, yet protect the power supply. The Fuel and Ox wires are to be monitored for current induced from the arc. The 30VDC power and return wires shall be positioned next to the Fuel and Ox coil wires in the bundle. All harnesses are fabricated and spot-tied with Nomex lacing cord per ML030-0013 and ML030-0014.

Harness No. 2 Configuration

See Figure E-2. The 30VDC power and return wires are twisted-pair 20AWG wires, approximately 16 inches long. The Fuel and Ox wires are two, twisted, shielded and jacketed pairs, and are to be monitored for current induced from the arc. The 30VDC power and return wires shall be positioned next to the Fuel and Ox coil wires in the bundle. All harnesses are fabricated and spot-tied with Nomex lacing cord per ML030-0013 and ML030-0014.

Harness No. 3 Configuration

See Figure E-1. The 30VDC power and return wires are twisted-pair 20AWG wires, approximately 16 inches long. The Fuel and Ox wires are two twisted, shielded and jacketed pairs with protective over wrap combinations called out in Table E-1 and are to be monitored for current induced from the arc. The 30VDC power and return wires shall be positioned next to the Fuel and Ox coil wires in the bundle. Install the protective over wrap configurations called out in Table E-1 per ML030-0014 and ML030-0013. All harnesses are fabricated and spot-tied with Nomex lacing cord per ML030-0013 and ML030-0014.

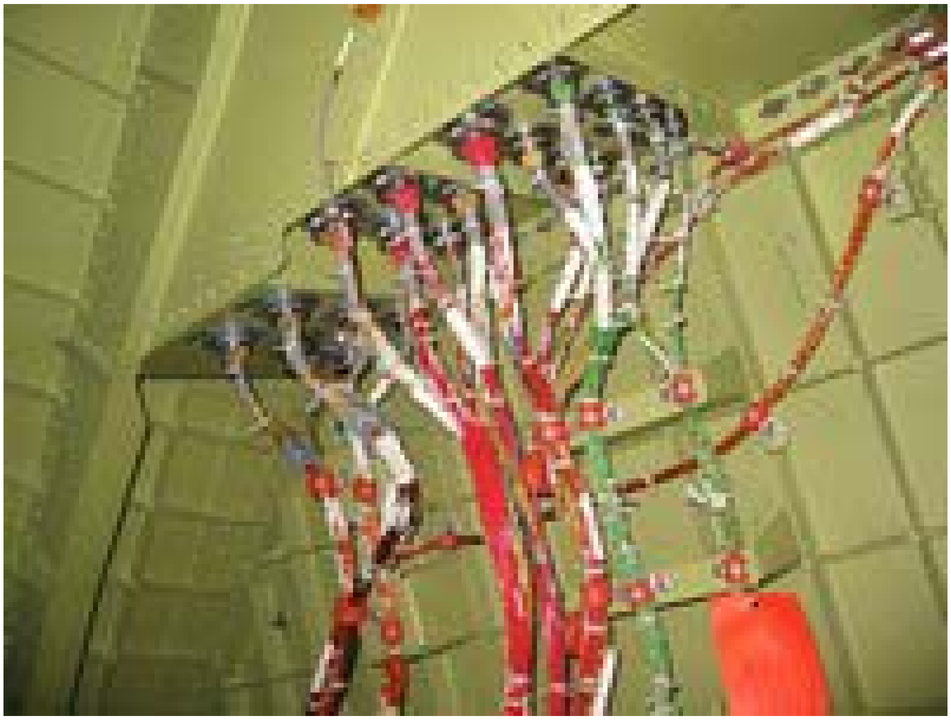


Figure E-1. Aft Engine Area

Harness No. 4 Configuration

See Figure E-2. The 30VDC power and return wires are twisted-pair 20AWG wires, approximately 16 inches long. The Fuel and Ox wires are two twisted pairs with protective over wrap combinations called out in Table E-1 and are to be monitored for current induced from the arc. The 30VDC power and return wires shall be positioned next to the Fuel and Ox coil wires in the bundle. Install the protective over wrap configurations called out in Table E-1 per ML030-0014 and ML030-0013. All harnesses are fabricated and spot-tied with Nomex lacing cord per ML030-0013 and ML030-0014.

Equipment

- Class II Primary Thruster Valve Assembly with mated flight connector and pigtail terminated with 4-pin connector (NESC to supply)
- Power supply, 30VDC, 20A
- Arc-Track testing machine (vibrating aluminum blade)
- Circuit protection fuses of appropriate size
- Chart recorder
- Video camera
- Camera with macro

Test Procedure

1. On each thruster harness, perform wet dielectric withstand voltage test per MIL-STD-2223 Method 3005.
2. Install Harness No. 1 into the Arc-Track testing machine.
3. Connect the Thruster Valve Assembly to both the Fuel coil and Ox coil wires via the pigtail 4-pin connector. Instrument the wires to measure current and voltage.
4. Abrade the 30VDC wire with the grounded blade from the Arc-Track testing machine, while vibrating the blade.
5. Record the current in the 30VDC supply circuits. Once an arc-track starts in a 30VDC twisted-pair wire, monitor and record any resultant current flow in the 11-ohm Fuel and Ox load wires.
6. Repeat Step 1.
7. Repeat test for four more sample harnesses (five total).
8. Repeat the above test on Harness No. 2, for five sample harnesses.

9. Repeat the above test on Harness No. 3, for five sample harnesses of each configuration in Table E-1 (60 total).

10. Repeat the above test on Harness No. 4, for five sample harnesses of each configuration in Table E-1 (60 total).

<table>
<tr><th colspan="2">TABLE E-1</th></tr>
<tr><td colspan="2">Harness No. 3 & 4 Over wrap Protection Schemes</td></tr>
<tr><td colspan="2">Fabricate per Space Shuttle Program wiring spec ML0303-0013 and ML0303-0014</td></tr>
<tr><td></td><td></td></tr>
<tr><td><b>First (or bottom) Layer</b></td><td><b>Second (or top) Layer</b></td></tr>
<tr><td>PTFE Wrap</td><td>None</td></tr>
<tr><td>Mystik 7503 Tape</td><td>None</td></tr>
<tr><td>Teflon Convoluted Tubing</td><td>None</td></tr>
<tr><td>PTFE Wrap</td><td>PTFE Wrap</td></tr>
<tr><td>PTFE Wrap</td><td>Mystik 7503 Tape</td></tr>
<tr><td>PTFE Wrap</td><td>Teflon Convoluted Tubing</td></tr>
<tr><td>Mystik 7503 Tape</td><td>PTFE Wrap</td></tr>
<tr><td>Mystic 7503 Tape</td><td>Mystik 7503 Tape</td></tr>
<tr><td>Mystik 7503 Tape</td><td>Teflon Convoluted Tubing</td></tr>
<tr><td>Teflon Convoluted Tubing</td><td>PTFE Wrap*</td></tr>
<tr><td>Teflon Convoluted Tubing</td><td>Mystik 7503 Tape*</td></tr>
<tr><td>Teflon Convoluted Tubing</td><td>Teflon Convoluted Tubing</td></tr>
</table>

* Note this protective over wrap configuration is not in the Shuttle spec. Follow same instructions of any 2 layer wrap with PTFE or Mystik 7503 tape as the second (or top) layer.

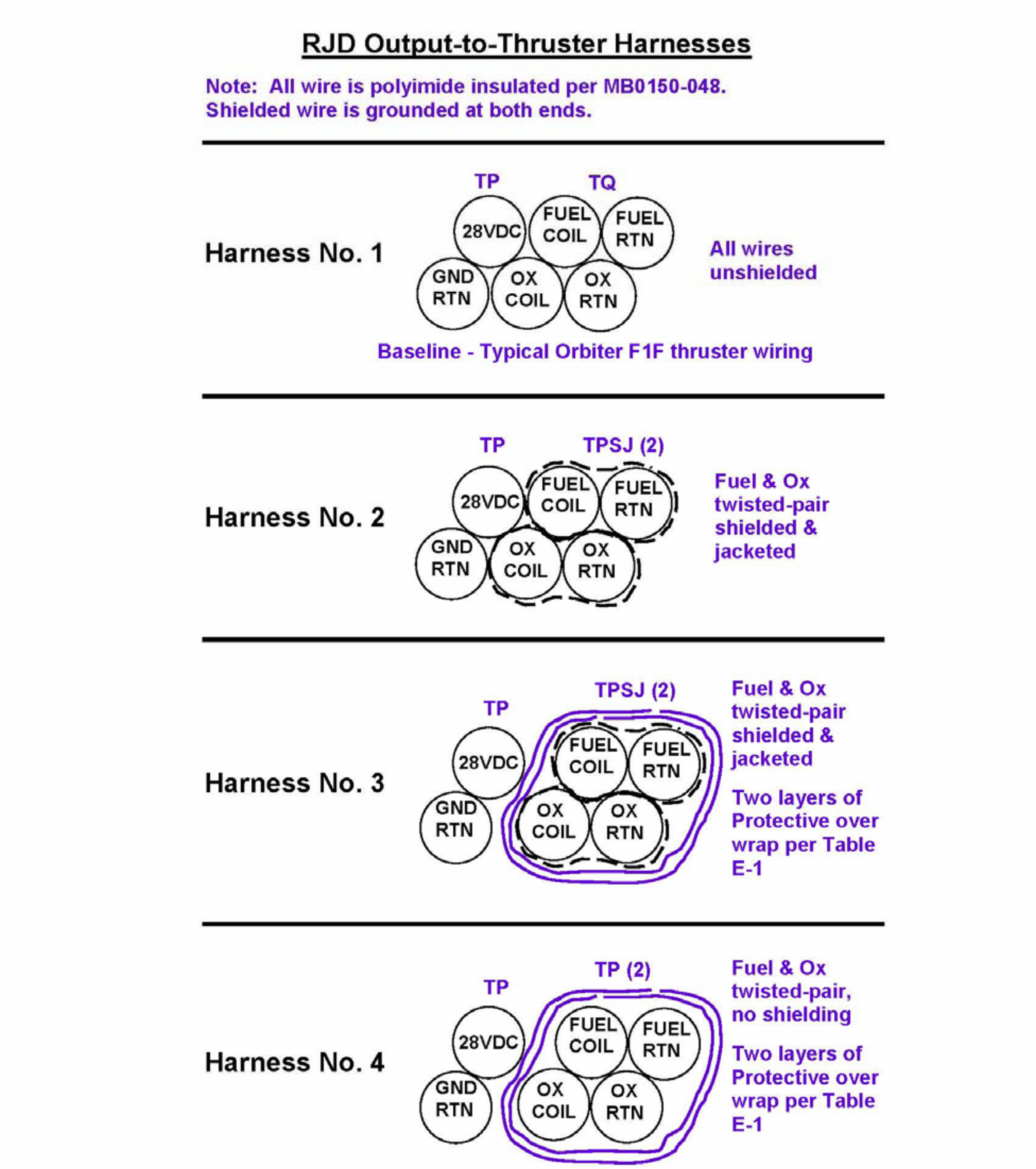
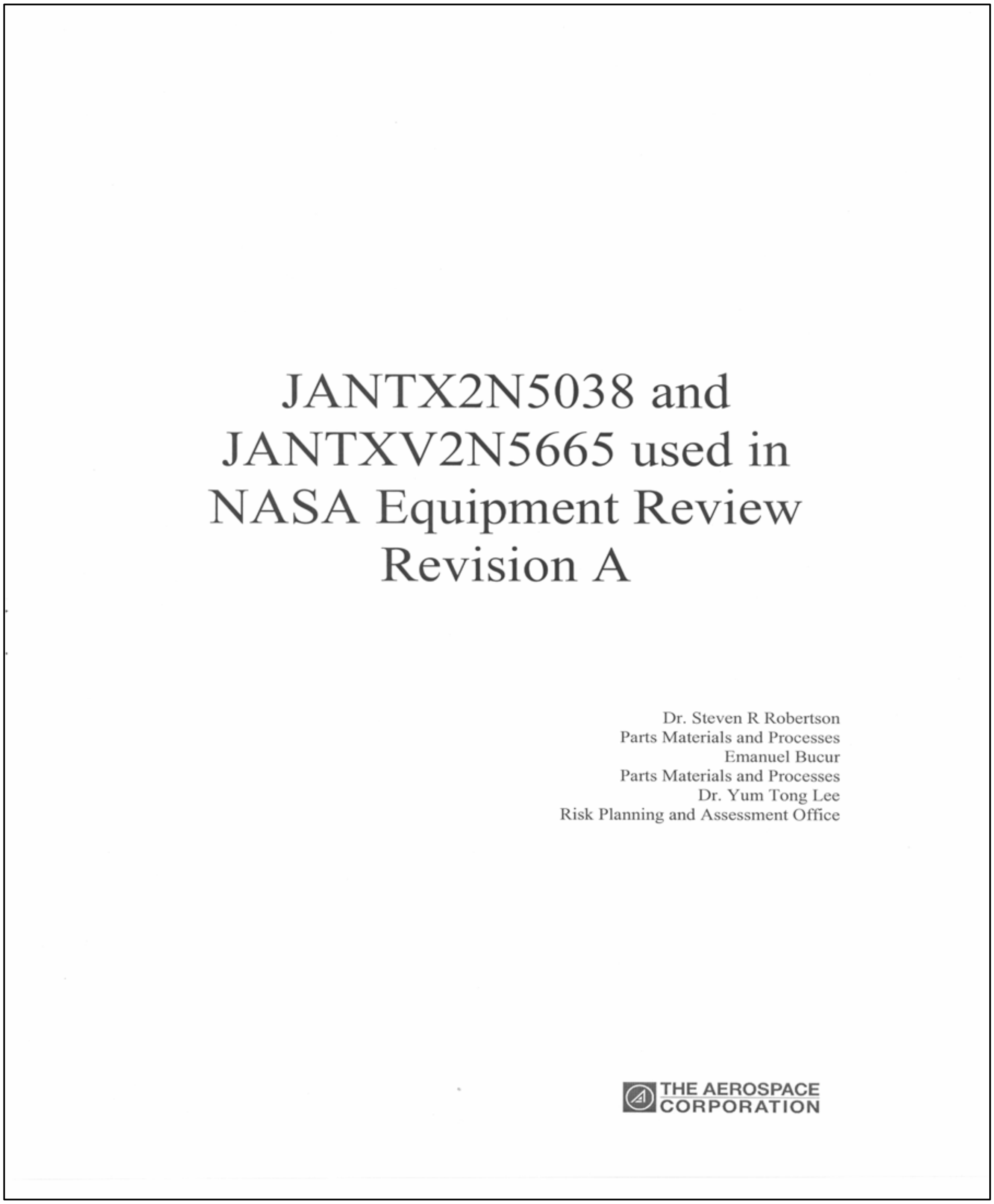

RJD Output-to-Thruster Harnesses
Note: All wire is polyimide insulated per MB0150-048.
Shielded wire is grounded at both ends.
Harness No. 1
TP
TQ
28VDC
FUEL COIL
FUEL RTN
GND RTN
OX COIL
OX RTN
All wires unshielded
Baseline - Typical Orbiter F1F thruster wiring
Harness No. 2
TP
TPSJ (2)
28VDC
FUEL COIL
FUEL RTN
GND RTN
OX COIL
OX RTN
Fuel & Ox twisted-pair shielded & jacketed
Harness No. 3
TP
TPSJ (2)
28VDC
FUEL COIL
FUEL RTN
GND RTN
OX COIL
OX RTN
Fuel & Ox twisted-pair shielded & jacketed
Two layers of Protective over wrap per Table E-1
Harness No. 4
TP
TP (2)
28VDC
FUEL COIL
FUEL RTN
GND RTN
OX COIL
OX RTN
Fuel & Ox twisted-pair, no shielding
Two layers of Protective over wrap per Table E-1

Figure E-2.
Note: Not all wires in each bundle are shown.

Appendix F

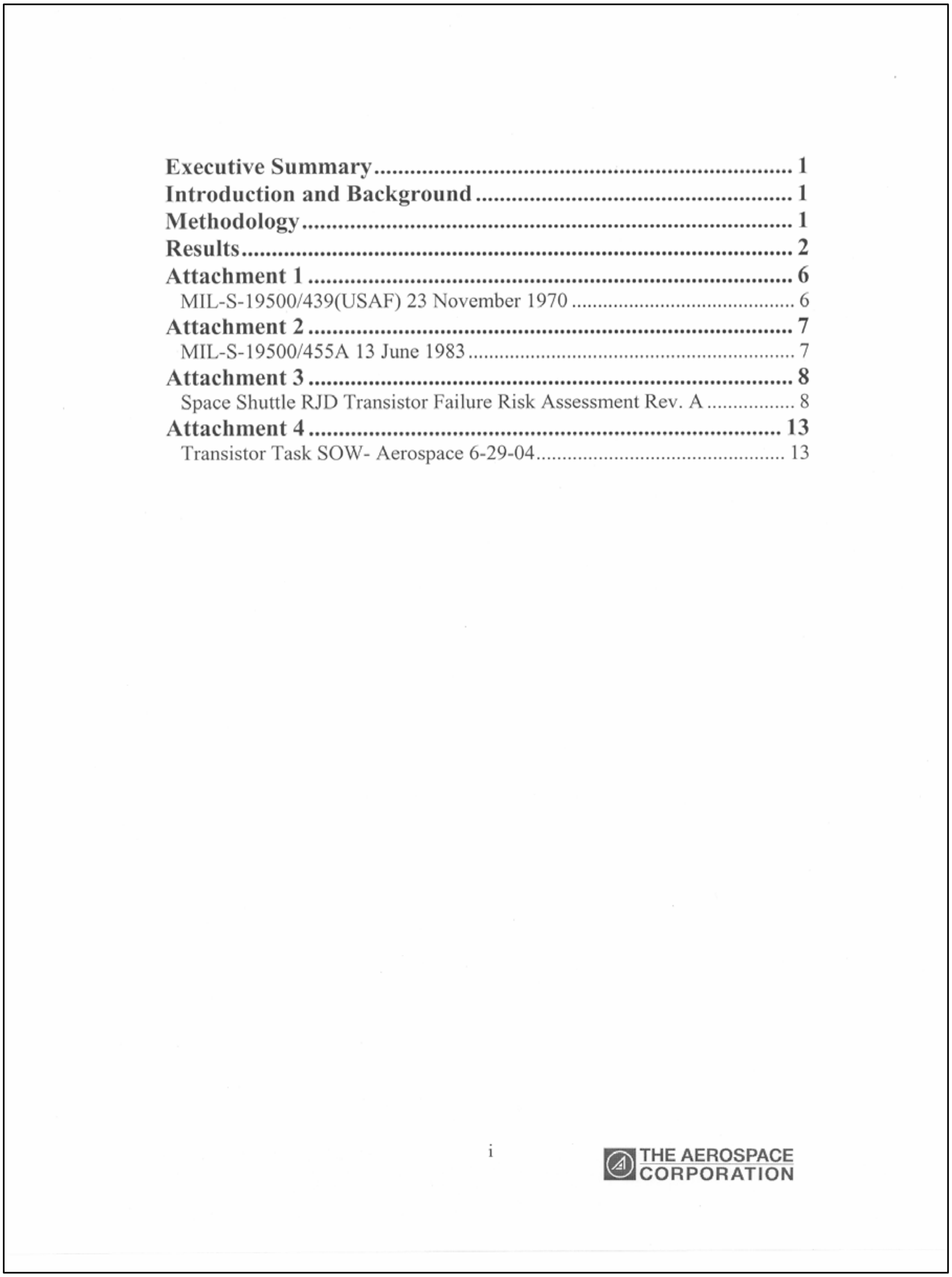
Aerospace Darlington Transistor Assessment Report



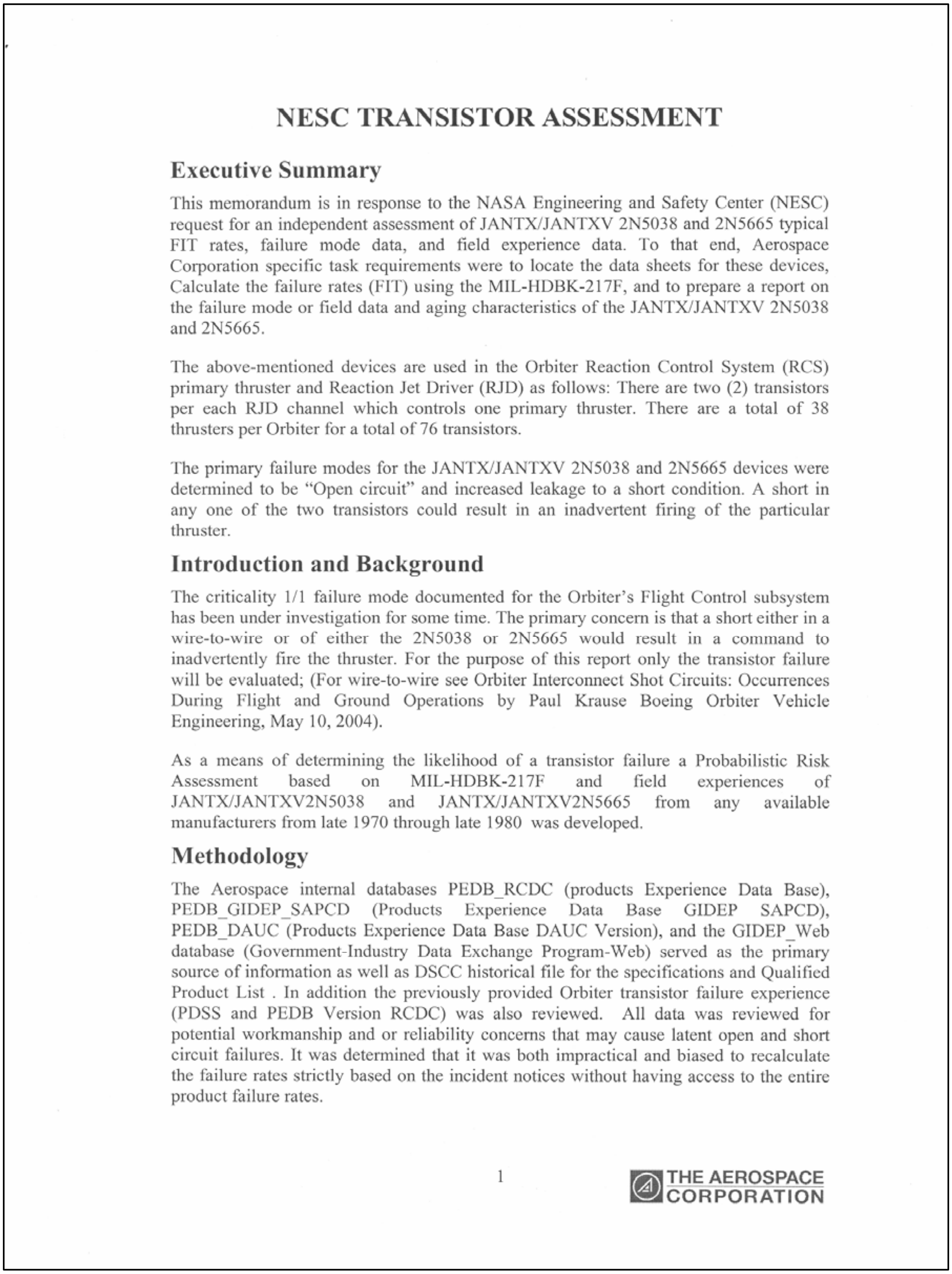
JANTX2N5038 and JANTXV2N5665 used in NASA Equipment Review Revision A

Dr. Steven R Robertson
Parts Materials and Processes
Emanuel Bucur
Parts Materials and Processes
Dr. Yum Tong Lee
Risk Planning and Assessment Office

THE AEROSPACE CORPORATION



Executive Summary **1**
Introduction and Background **1**
Methodology **1**
Results **2**
Attachment 1 .... **6**
MIL-S-19500/439(USAF) 23 November 1970 6
Attachment 2 .... **7**
MIL-S-19500/455A 13 June 1983 7
Attachment 3 .... **8**
Space Shuttle RJD Transistor Failure Risk Assessment Rev. A 8
Attachment 4 .... **13**
Transistor Task SOW- Aerospace 6-29-04 13



NESC TRANSISTOR ASSESSMENT

Executive Summary

This memorandum is in response to the NASA Engineering and Safety Center (NESC) request for an independent assessment of JANTX/JANTXV 2N5038 and 2N5665 typical FIT rates, failure mode data, and field experience data. To that end, Aerospace Corporation specific task requirements were to locate the data sheets for these devices, Calculate the failure rates (FIT) using the MIL-HDBK-217F, and to prepare a report on the failure mode or field data and aging characteristics of the JANTX/JANTXV 2N5038 and 2N5665.

The above-mentioned devices are used in the Orbiter Reaction Control System (RCS) primary thruster and Reaction Jet Driver (RJD) as follows: There are two (2) transistors per each RJD channel which controls one primary thruster. There are a total of 38 thrusters per Orbiter for a total of 76 transistors.

The primary failure modes for the JANTX/JANTXV 2N5038 and 2N5665 devices were determined to be "Open circuit" and increased leakage to a short condition. A short in any one of the two transistors could result in an inadvertent firing of the particular thruster.

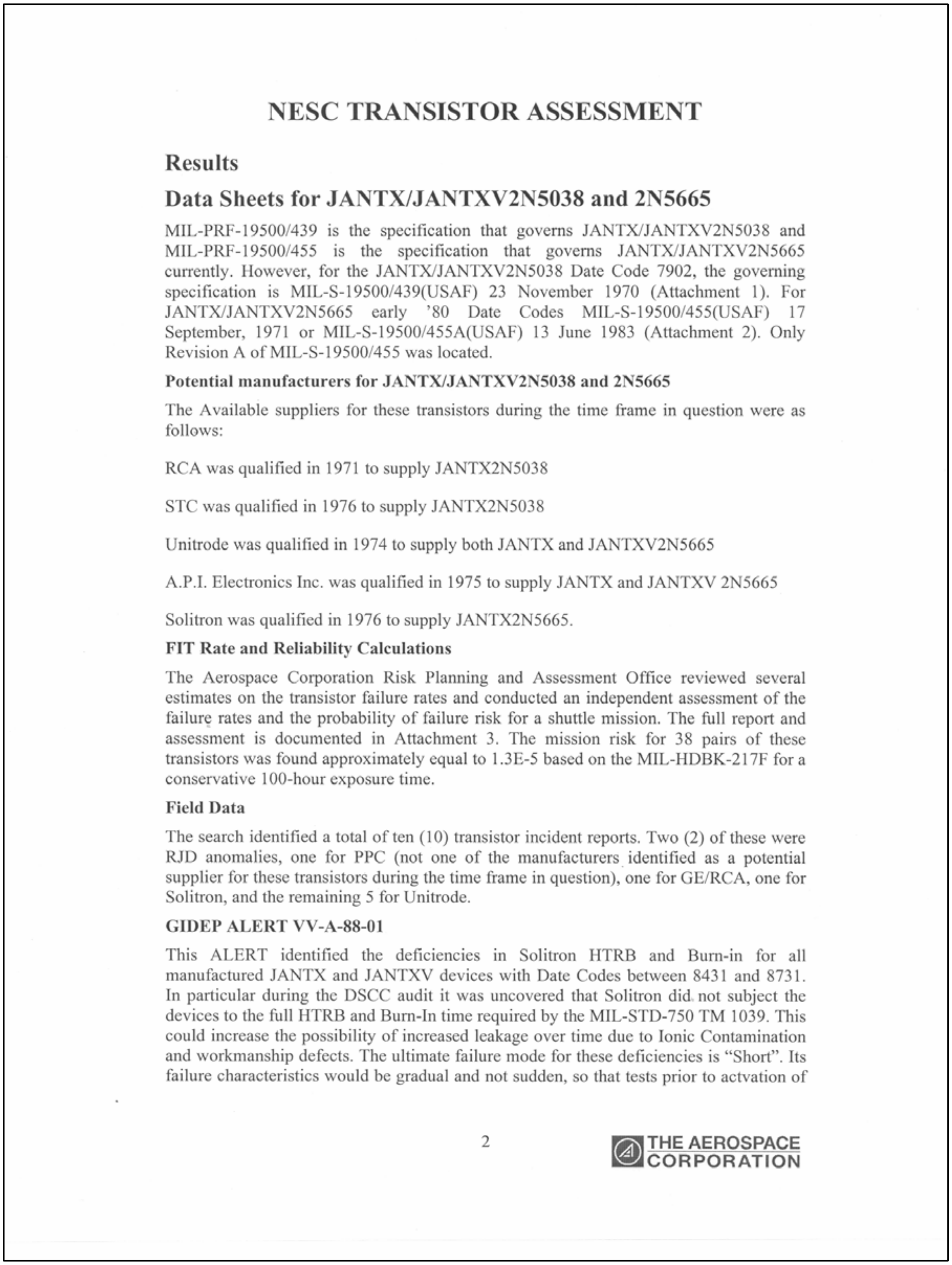
Introduction and Background

The criticality 1/1 failure mode documented for the Orbiter's Flight Control subsystem has been under investigation for some time. The primary concern is that a short either in a wire-to-wire or of either the 2N5038 or 2N5665 would result in a command to inadvertently fire the thruster. For the purpose of this report only the transistor failure will be evaluated; (For wire-to-wire see Orbiter Interconnect Shot Circuits: Occurrences During Flight and Ground Operations by Paul Krause Boeing Orbiter Vehicle Engineering, May 10, 2004).

As a means of determining the likelihood of a transistor failure a Probabilistic Risk Assessment based on MIL-HDBK-217F and field experiences of JANTX/JANTXV2N5038 and JANTX/JANTXV2N5665 from any available manufacturers from late 1970 through late 1980 was developed.

Methodology

The Aerospace internal databases PEDB_RCDC (products Experience Data Base), PEDB_GIDEP_SAPCD (Products Experience Data Base GIDEP SAPCD), PEDB_DAUC (Products Experience Data Base DAUC Version), and the GIDEP_Web database (Government-Industry Data Exchange Program-Web) served as the primary source of information as well as DSCC historical file for the specifications and Qualified Product List . In addition the previously provided Orbiter transistor failure experience (PDSS and PEDB Version RCDC) was also reviewed. All data was reviewed for potential workmanship and or reliability concerns that may cause latent open and short circuit failures. It was determined that it was both impractical and biased to recalculate the failure rates strictly based on the incident notices without having access to the entire product failure rates.



NESC TRANSISTOR ASSESSMENT

Results

Data Sheets for JANTX/JANTXV2N5038 and 2N5665

MIL-PRF-19500/439 is the specification that governs JANTX/JANTXV2N5038 and MIL-PRF-19500/455 is the specification that governs JANTX/JANTXV2N5665 currently. However, for the JANTX/JANTXV2N5038 Date Code 7902, the governing specification is MIL-S-19500/439(USAF) 23 November 1970 (Attachment 1). For JANTX/JANTXV2N5665 early '80 Date Codes MIL-S-19500/455(USAF) 17 September, 1971 or MIL-S-19500/455A(USAF) 13 June 1983 (Attachment 2). Only Revision A of MIL-S-19500/455 was located.

Potential manufacturers for JANTX/JANTXV2N5038 and 2N5665

The Available suppliers for these transistors during the time frame in question were as follows:

RCA was qualified in 1971 to supply JANTX2N5038

STC was qualified in 1976 to supply JANTX2N5038

Unitrode was qualified in 1974 to supply both JANTX and JANTXV2N5665

A.P.I. Electronics Inc. was qualified in 1975 to supply JANTX and JANTXV 2N5665

Solitron was qualified in 1976 to supply JANTX2N5665.

FIT Rate and Reliability Calculations

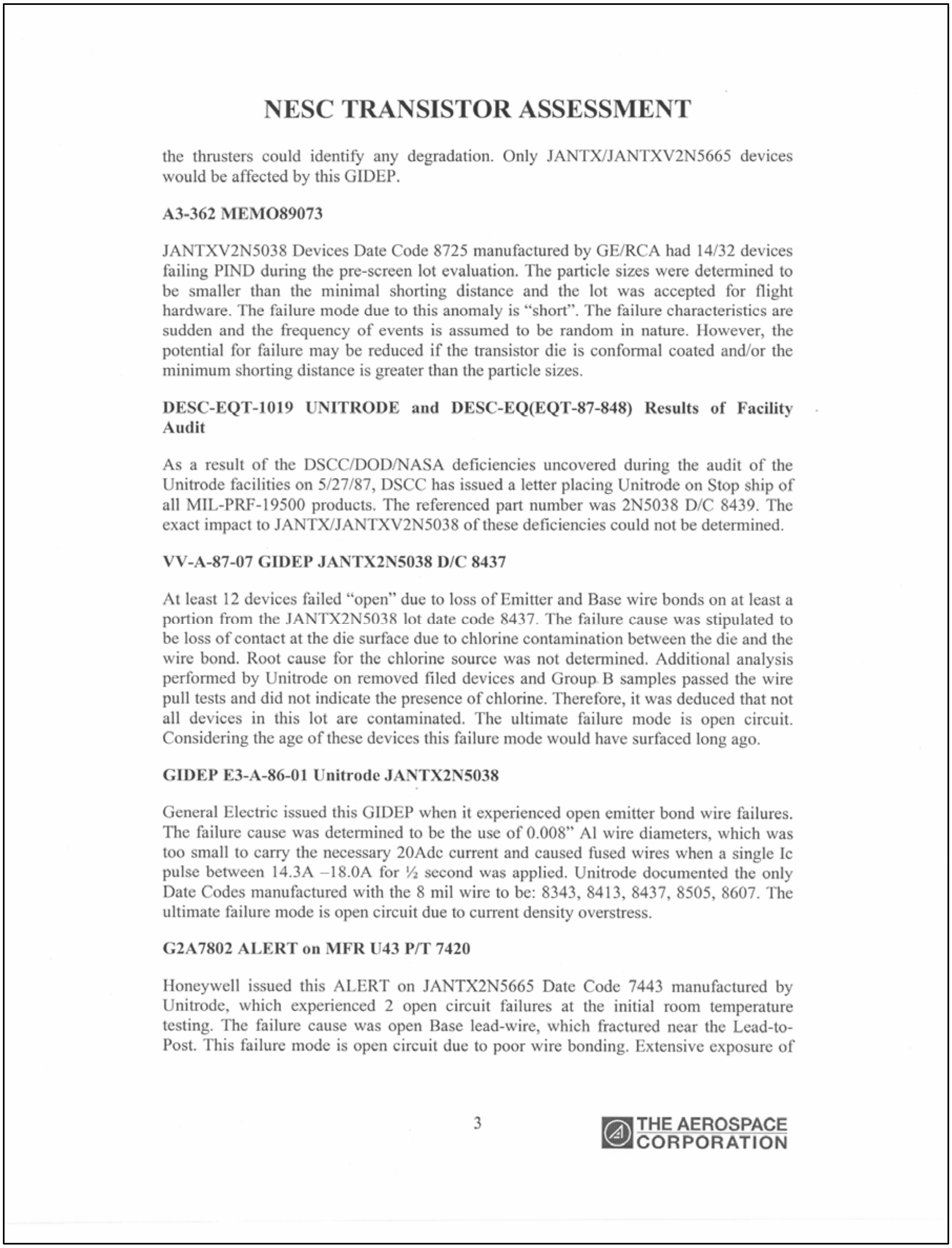
The Aerospace Corporation Risk Planning and Assessment Office reviewed several estimates on the transistor failure rates and conducted an independent assessment of the failure rates and the probability of failure risk for a shuttle mission. The full report and assessment is documented in Attachment 3. The mission risk for 38 pairs of these transistors was found approximately equal to 1.3E-5 based on the MIL-HDBK-217F for a conservative 100-hour exposure time.

Field Data

The search identified a total of ten (10) transistor incident reports. Two (2) of these were RJD anomalies, one for PPC (not one of the manufacturers identified as a potential supplier for these transistors during the time frame in question), one for GE/RCA, one for Solitron, and the remaining 5 for Unitrode.

GIDEP ALERT VV-A-88-01

This ALERT identified the deficiencies in Solitron HTRB and Burn-in for all manufactured JANTX and JANTXV devices with Date Codes between 8431 and 8731. In particular during the DSCC audit it was uncovered that Solitron did not subject the devices to the full HTRB and Burn-In time required by the MIL-STD-750 TM 1039. This could increase the possibility of increased leakage over time due to Ionic Contamination and workmanship defects. The ultimate failure mode for these deficiencies is "Short". Its failure characteristics would be gradual and not sudden, so that tests prior to actvation of



the thrusters could identify any degradation. Only JANTX/JANTXV2N5665 devices would be affected by this GIDEP.

A3-362 MEMO89073

JANTXV2N5038 Devices Date Code 8725 manufactured by GE/RCA had 14/32 devices failing PIND during the pre-screen lot evaluation. The particle sizes were determined to be smaller than the minimal shorting distance and the lot was accepted for flight hardware. The failure mode due to this anomaly is "short". The failure characteristics are sudden and the frequency of events is assumed to be random in nature. However, the potential for failure may be reduced if the transistor die is conformal coated and/or the minimum shorting distance is greater than the particle sizes.

DESC-EQT-1019 UNITRODE and DESC-EQ(EQT-87-848) Results of Facility Audit

As a result of the DSCC/DOD/NASA deficiencies uncovered during the audit of the Unitrode facilities on 5/27/87, DSCC has issued a letter placing Unitrode on Stop ship of all MIL-PRF-19500 products. The referenced part number was 2N5038 D/C 8439. The exact impact to JANTX/JANTXV2N5038 of these deficiencies could not be determined.

VV-A-87-07 GIDEP JANTX2N5038 D/C 8437

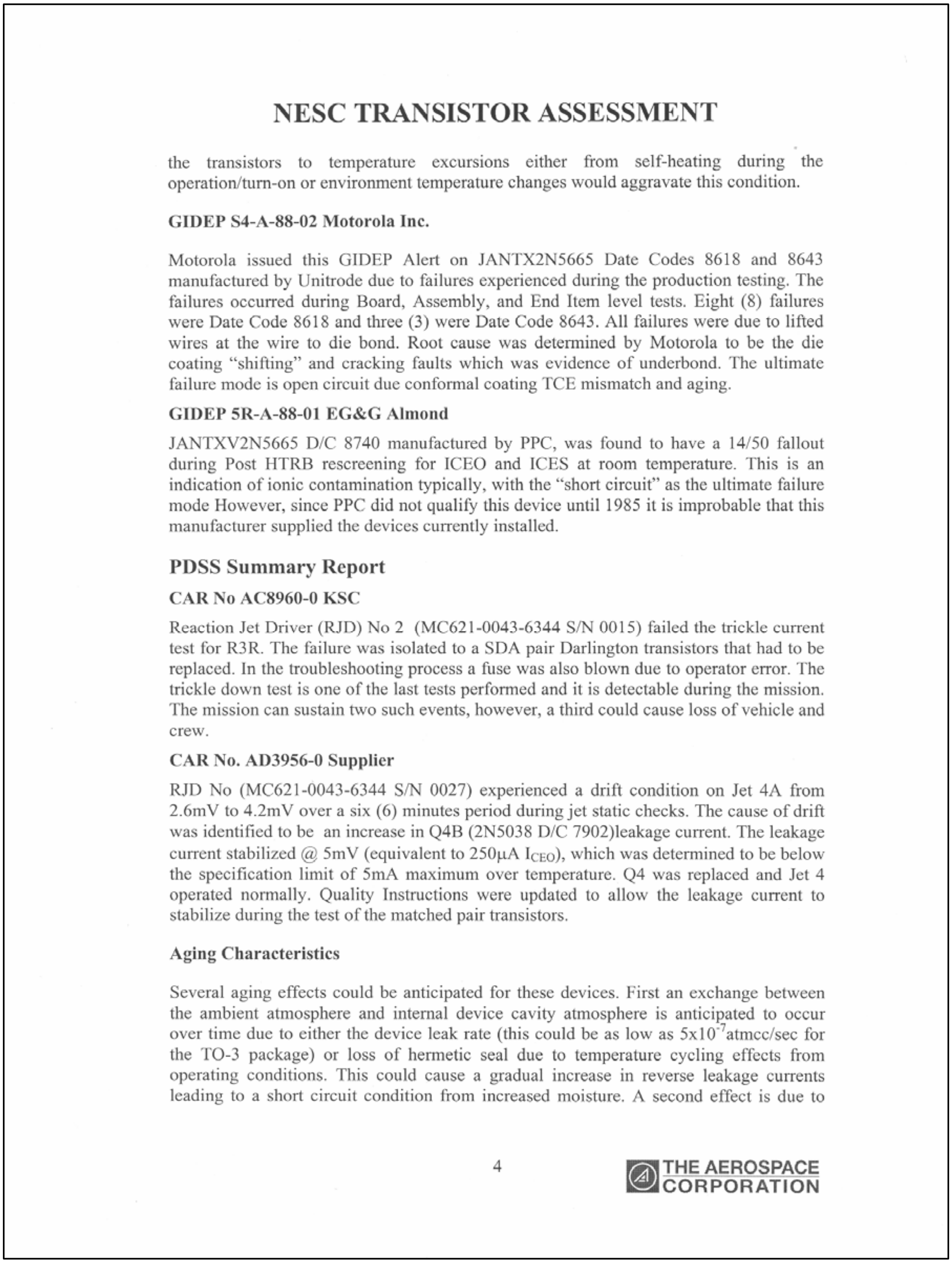
At least 12 devices failed "open" due to loss of Emitter and Base wire bonds on at least a portion from the JANTX2N5038 lot date code 8437. The failure cause was stipulated to be loss of contact at the die surface due to chlorine contamination between the die and the wire bond. Root cause for the chlorine source was not determined. Additional analysis performed by Unitrode on removed filed devices and Group B samples passed the wire pull tests and did not indicate the presence of chlorine. Therefore, it was deduced that not all devices in this lot are contaminated. The ultimate failure mode is open circuit. Considering the age of these devices this failure mode would have surfaced long ago.

GIDEP E3-A-86-01 Unitrode JANTX2N5038

General Electric issued this GIDEP when it experienced open emitter bond wire failures. The failure cause was determined to be the use of 0.008" Al wire diameters, which was too small to carry the necessary 20Adc current and caused fused wires when a single Ic pulse between 14.3A –18.0A for ½ second was applied. Unitrode documented the only Date Codes manufactured with the 8 mil wire to be: 8343, 8413, 8437, 8505, 8607. The ultimate failure mode is open circuit due to current density overstress.

G2A7802 ALERT on MFR U43 P/T 7420

Honeywell issued this ALERT on JANTX2N5665 Date Code 7443 manufactured by Unitrode, which experienced 2 open circuit failures at the initial room temperature testing. The failure cause was open Base lead-wire, which fractured near the Lead-to-Post. This failure mode is open circuit due to poor wire bonding. Extensive exposure of



the transistors to temperature excursions either from self-heating during the operation/turn-on or environment temperature changes would aggravate this condition.

GIDEP S4-A-88-02 Motorola Inc.

Motorola issued this GIDEP Alert on JANTX2N5665 Date Codes 8618 and 8643 manufactured by Unitrode due to failures experienced during the production testing. The failures occurred during Board, Assembly, and End Item level tests. Eight (8) failures were Date Code 8618 and three (3) were Date Code 8643. All failures were due to lifted wires at the wire to die bond. Root cause was determined by Motorola to be the die coating "shifting" and cracking faults which was evidence of underbond. The ultimate failure mode is open circuit due conformal coating TCE mismatch and aging.

GIDEP 5R-A-88-01 EG&G Almond

JANTXV2N5665 D/C 8740 manufactured by PPC, was found to have a 14/50 fallout during Post HTRB rescreening for ICEO and ICES at room temperature. This is an indication of ionic contamination typically, with the "short circuit" as the ultimate failure mode However, since PPC did not qualify this device until 1985 it is improbable that this manufacturer supplied the devices currently installed.

PDSS Summary Report

CAR No AC8960-0 KSC

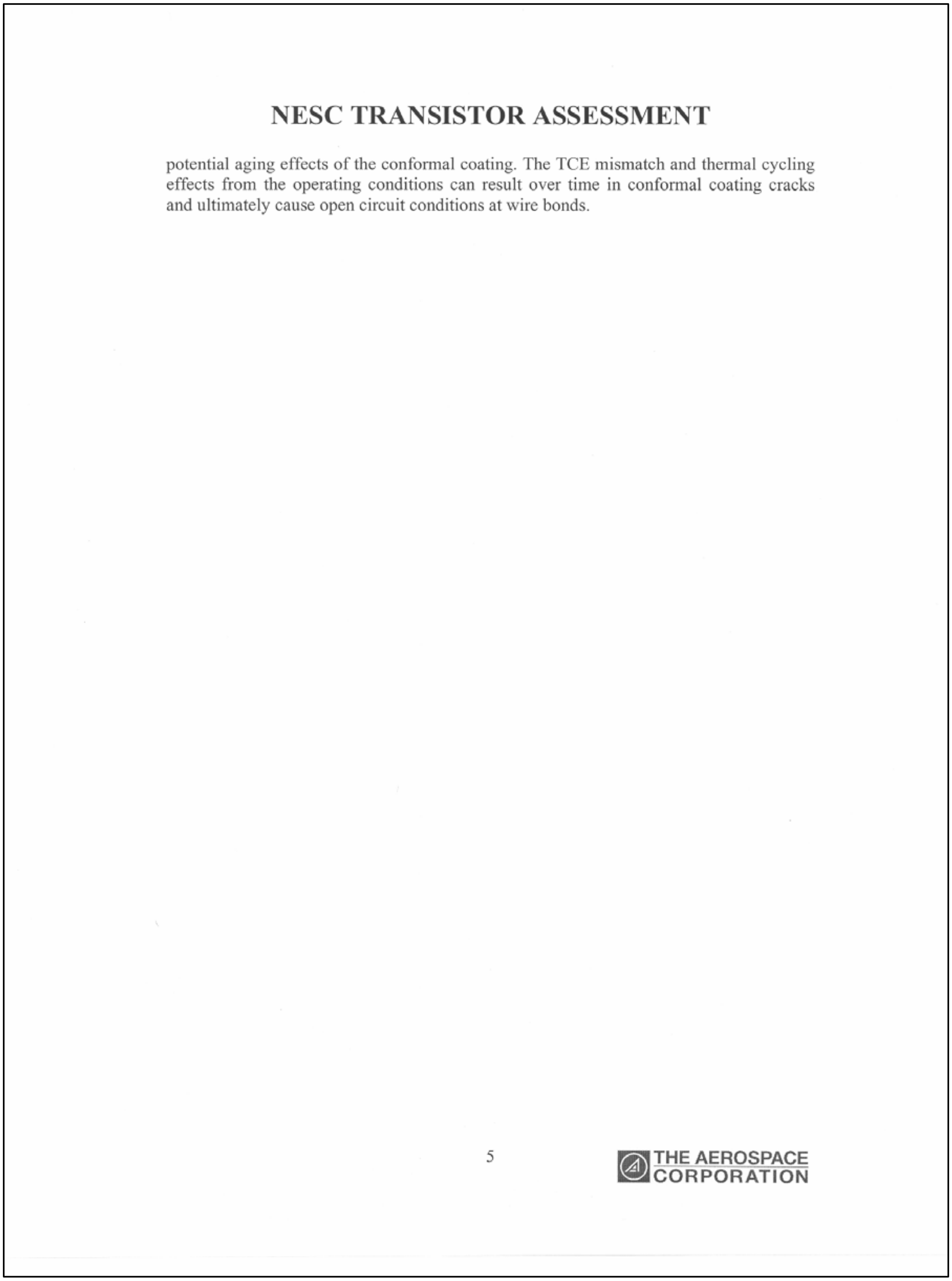
Reaction Jet Driver (RJD) No 2 (MC621-0043-6344 S/N 0015) failed the trickle current test for R3R. The failure was isolated to a SDA pair Darlington transistors that had to be replaced. In the troubleshooting process a fuse was also blown due to operator error. The trickle down test is one of the last tests performed and it is detectable during the mission. The mission can sustain two such events, however, a third could cause loss of vehicle and crew.

CAR No. AD3956-0 Supplier

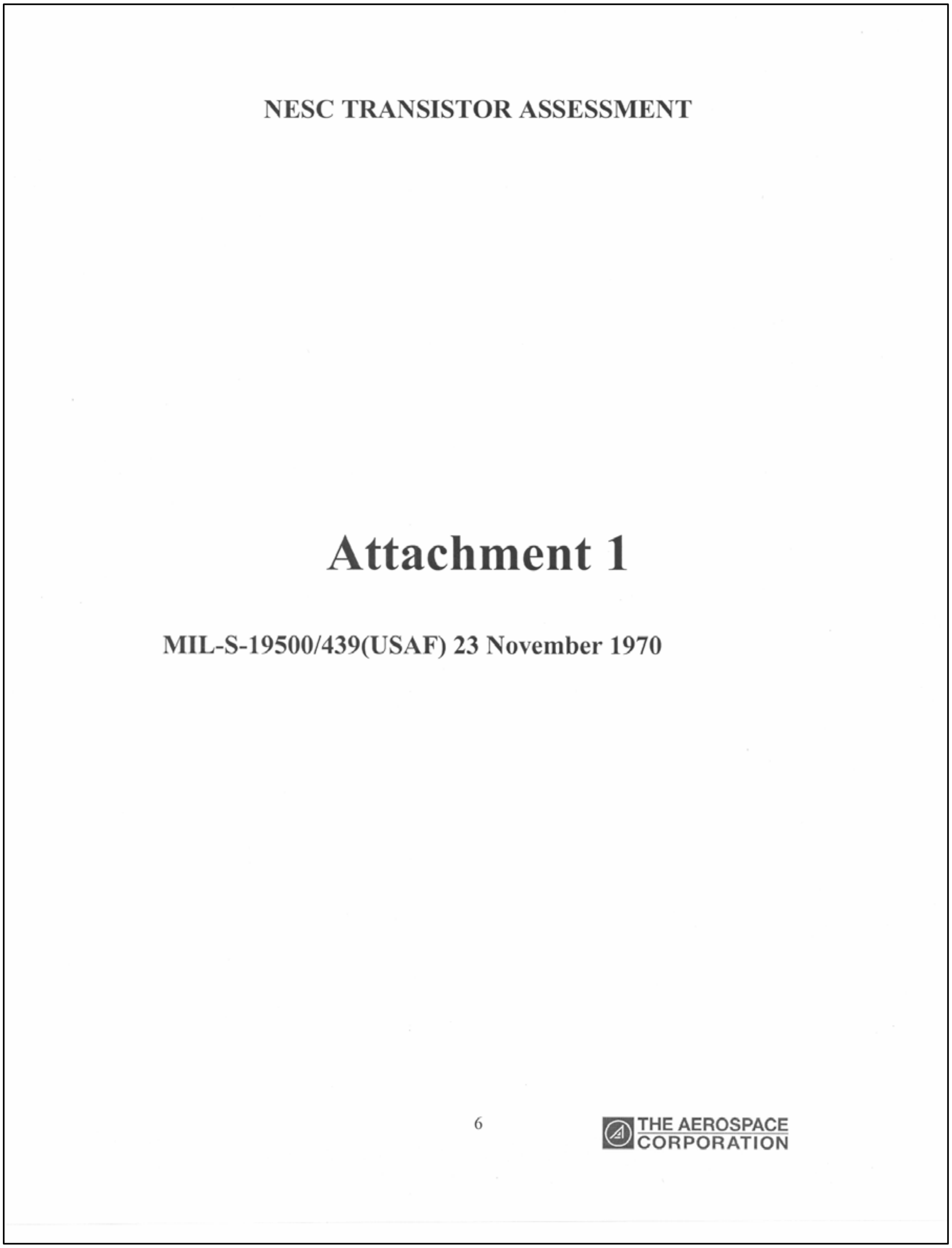
RJD No (MC621-0043-6344 S/N 0027) experienced a drift condition on Jet 4A from 2.6mV to 4.2mV over a six (6) minutes period during jet static checks. The cause of drift was identified to be an increase in Q4B (2N5038 D/C 7902)leakage current. The leakage current stabilized @ 5mV (equivalent to 250μA I_{CEO}), which was determined to be below the specification limit of 5mA maximum over temperature. Q4 was replaced and Jet 4 operated normally. Quality Instructions were updated to allow the leakage current to stabilize during the test of the matched pair transistors.

Aging Characteristics

Several aging effects could be anticipated for these devices. First an exchange between the ambient atmosphere and internal device cavity atmosphere is anticipated to occur over time due to either the device leak rate (this could be as low as $5x10^{-7}$atmcc/sec for the TO-3 package) or loss of hermetic seal due to temperature cycling effects from operating conditions. This could cause a gradual increase in reverse leakage currents leading to a short circuit condition from increased moisture. A second effect is due to

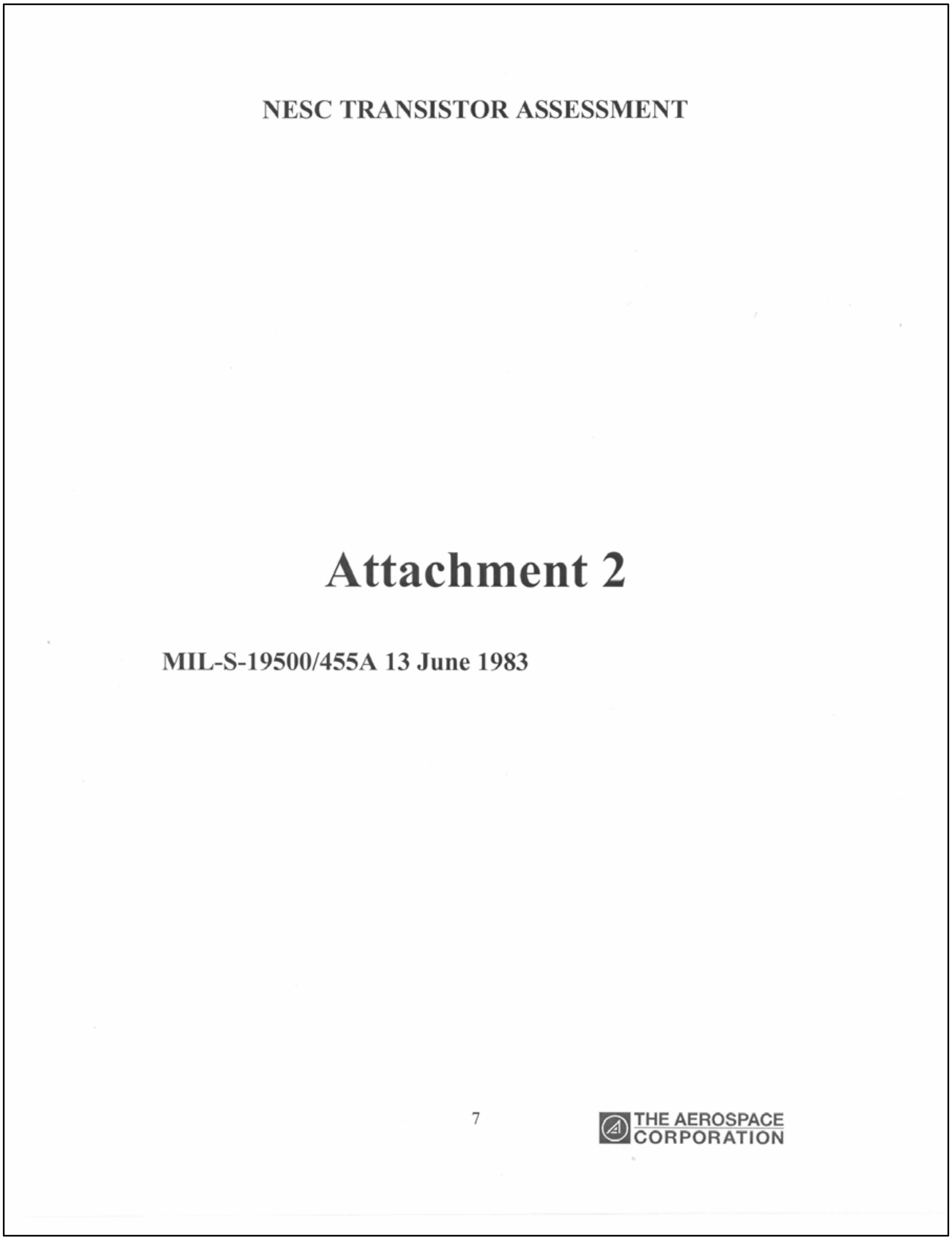


potential aging effects of the conformal coating. The TCE mismatch and thermal cycling effects from the operating conditions can result over time in conformal coating cracks and ultimately cause open circuit conditions at wire bonds.



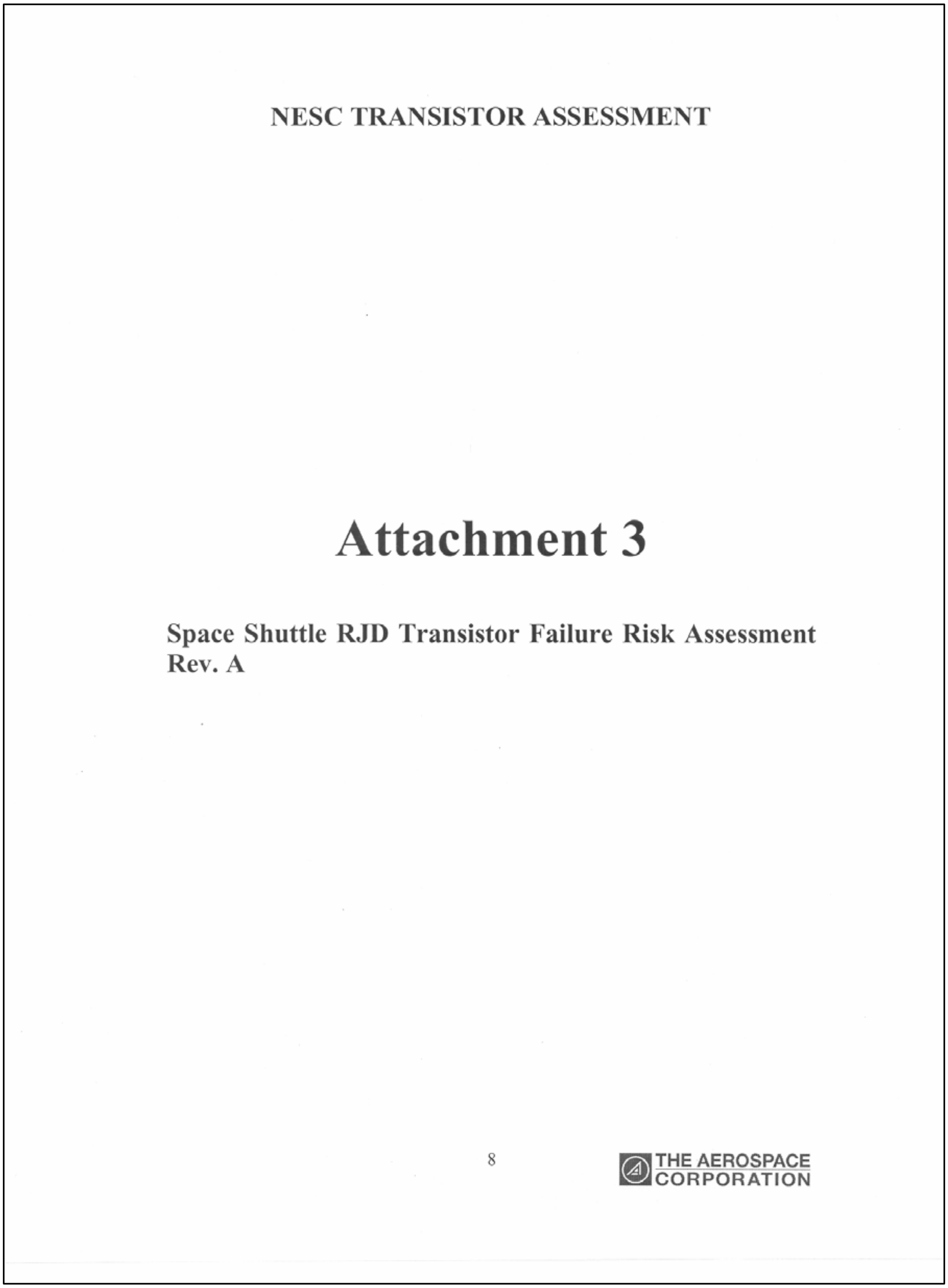
Attachment 1

MIL-S-19500/439(USAF) 23 November 1970



Attachment 2

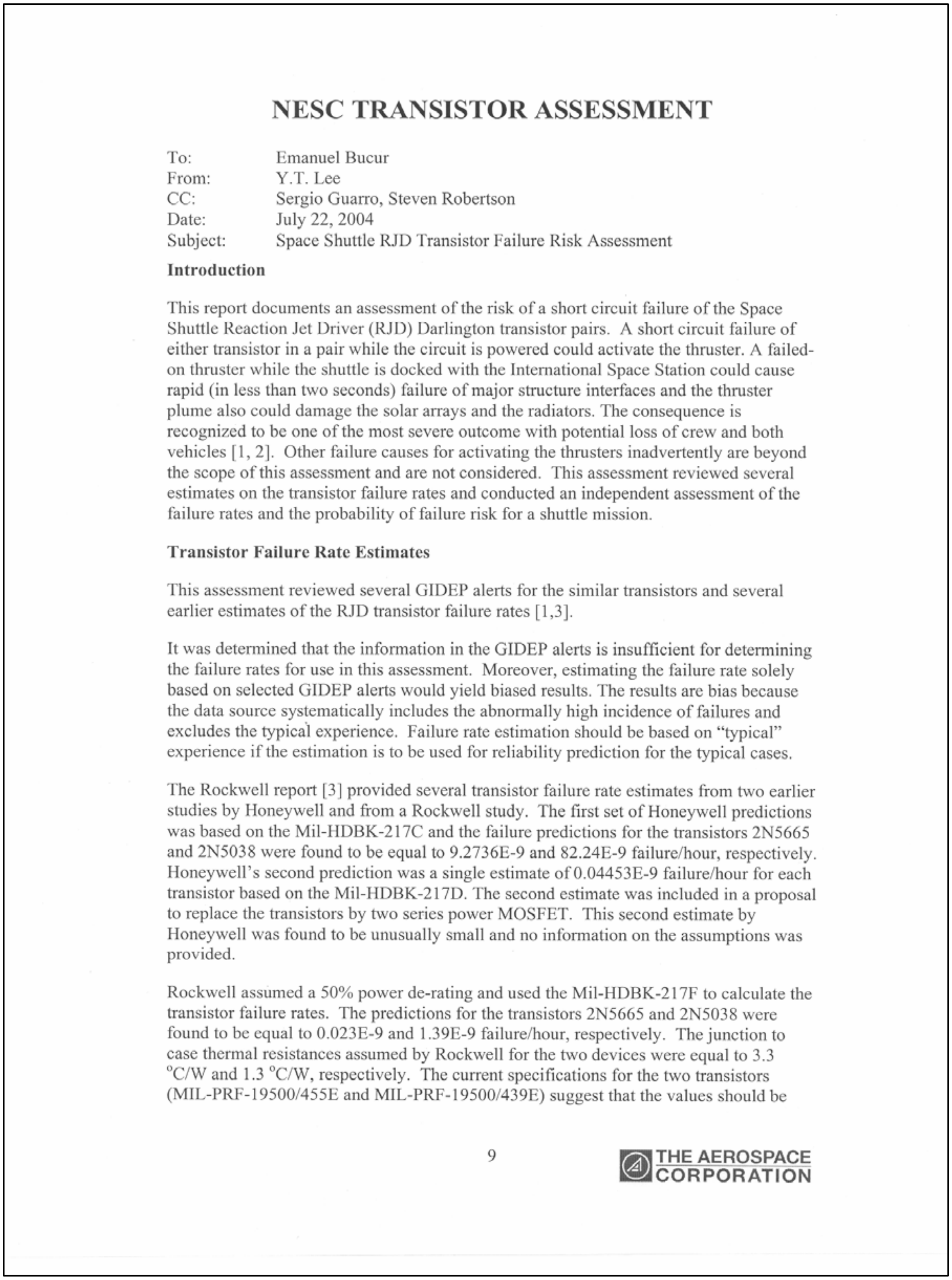
MIL-S-19500/455A 13 June 1983



NESC TRANSISTOR ASSESSMENT

Attachment 3

Space Shuttle RJD Transistor Failure Risk Assessment Rev. A



NESC TRANSISTOR ASSESSMENT

To:	Emanuel Bucur
From:	Y.T. Lee
CC:	Sergio Guarro, Steven Robertson
Date:	July 22, 2004
Subject:	Space Shuttle RJD Transistor Failure Risk Assessment

Introduction

This report documents an assessment of the risk of a short circuit failure of the Space Shuttle Reaction Jet Driver (RJD) Darlington transistor pairs. A short circuit failure of either transistor in a pair while the circuit is powered could activate the thruster. A failed-on thruster while the shuttle is docked with the International Space Station could cause rapid (in less than two seconds) failure of major structure interfaces and the thruster plume also could damage the solar arrays and the radiators. The consequence is recognized to be one of the most severe outcome with potential loss of crew and both vehicles [1, 2]. Other failure causes for activating the thrusters inadvertently are beyond the scope of this assessment and are not considered. This assessment reviewed several estimates on the transistor failure rates and conducted an independent assessment of the failure rates and the probability of failure risk for a shuttle mission.

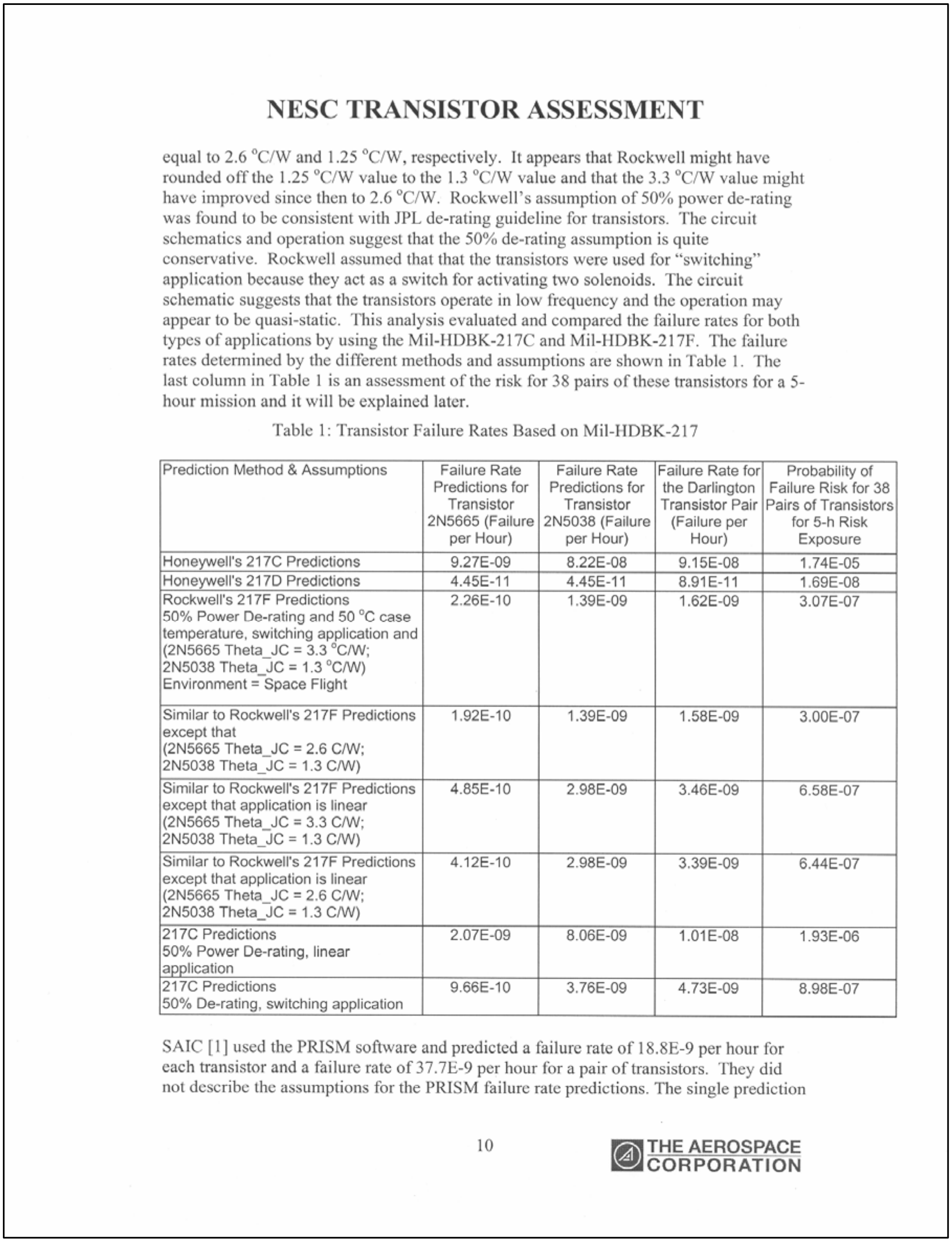
Transistor Failure Rate Estimates

This assessment reviewed several GIDEP alerts for the similar transistors and several earlier estimates of the RJD transistor failure rates [1,3].

It was determined that the information in the GIDEP alerts is insufficient for determining the failure rates for use in this assessment. Moreover, estimating the failure rate solely based on selected GIDEP alerts would yield biased results. The results are bias because the data source systematically includes the abnormally high incidence of failures and excludes the typical experience. Failure rate estimation should be based on "typical" experience if the estimation is to be used for reliability prediction for the typical cases.

The Rockwell report [3] provided several transistor failure rate estimates from two earlier studies by Honeywell and from a Rockwell study. The first set of Honeywell predictions was based on the Mil-HDBK-217C and the failure predictions for the transistors 2N5665 and 2N5038 were found to be equal to 9.2736E-9 and 82.24E-9 failure/hour, respectively. Honeywell's second prediction was a single estimate of 0.04453E-9 failure/hour for each transistor based on the Mil-HDBK-217D. The second estimate was included in a proposal to replace the transistors by two series power MOSFET. This second estimate by Honeywell was found to be unusually small and no information on the assumptions was provided.

Rockwell assumed a 50% power de-rating and used the Mil-HDBK-217F to calculate the transistor failure rates. The predictions for the transistors 2N5665 and 2N5038 were found to be equal to 0.023E-9 and 1.39E-9 failure/hour, respectively. The junction to case thermal resistances assumed by Rockwell for the two devices were equal to 3.3 °C/W and 1.3 °C/W, respectively. The current specifications for the two transistors (MIL-PRF-19500/455E and MIL-PRF-19500/439E) suggest that the values should be

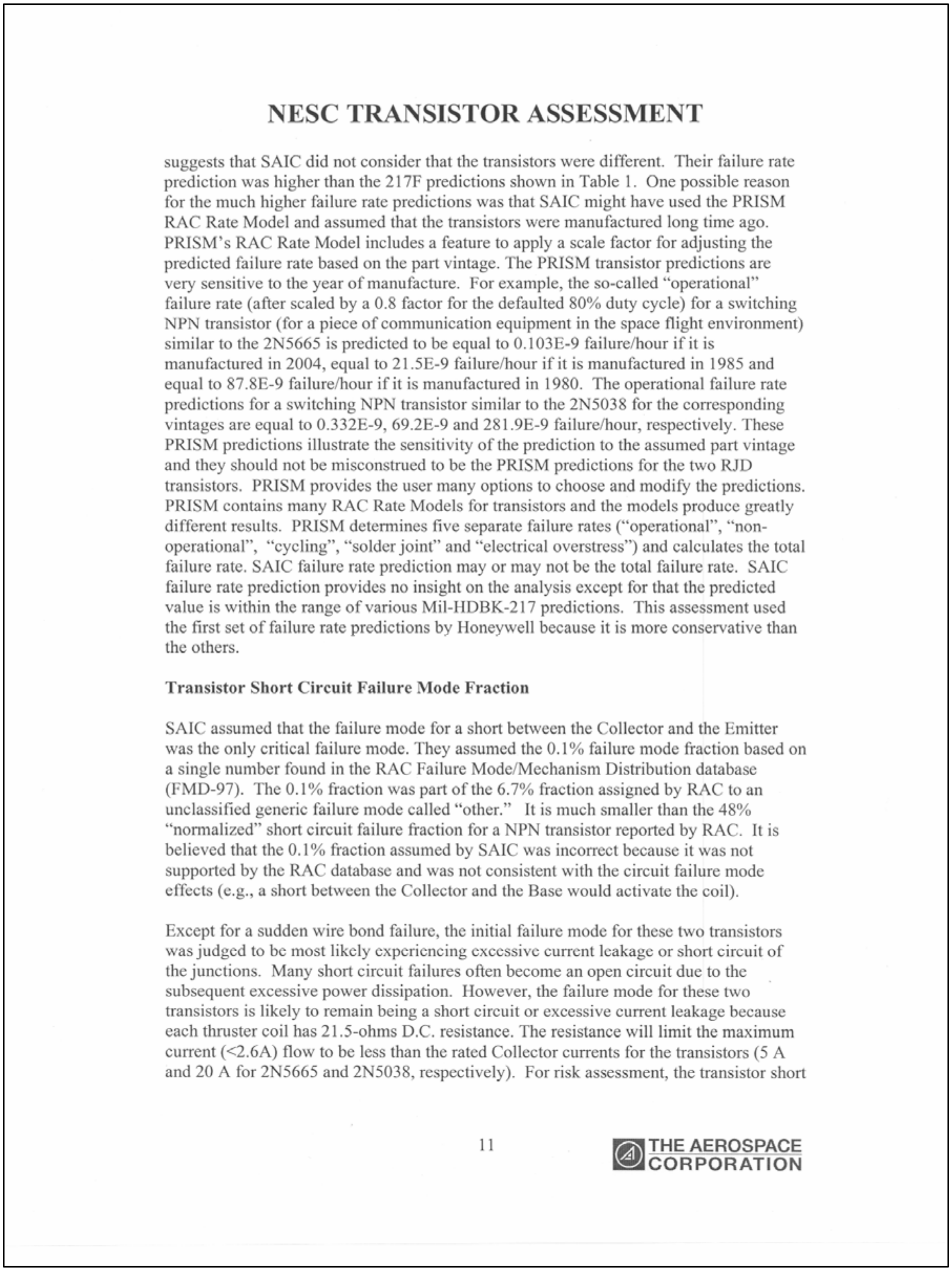


equal to 2.6 °C/W and 1.25 °C/W, respectively. It appears that Rockwell might have rounded off the 1.25 °C/W value to the 1.3 °C/W value and that the 3.3 °C/W value might have improved since then to 2.6 °C/W. Rockwell's assumption of 50% power de-rating was found to be consistent with JPL de-rating guideline for transistors. The circuit schematics and operation suggest that the 50% de-rating assumption is quite conservative. Rockwell assumed that that the transistors were used for "switching" application because they act as a switch for activating two solenoids. The circuit schematic suggests that the transistors operate in low frequency and the operation may appear to be quasi-static. This analysis evaluated and compared the failure rates for both types of applications by using the Mil-HDBK-217C and Mil-HDBK-217F. The failure rates determined by the different methods and assumptions are shown in Table 1. The last column in Table 1 is an assessment of the risk for 38 pairs of these transistors for a 5-hour mission and it will be explained later.

Table 1: Transistor Failure Rates Based on Mil-HDBK-217

Prediction Method & Assumptions	Failure Rate Predictions for Transistor 2N5665 (Failure per Hour)	Failure Rate Predictions for Transistor 2N5038 (Failure per Hour)	Failure Rate for the Darlington Transistor Pair (Failure per Hour)	Probability of Failure Risk for 38 Pairs of Transistors for 5-h Risk Exposure
Honeywell's 217C Predictions	9.27E-09	8.22E-08	9.15E-08	1.74E-05
Honeywell's 217D Predictions	4.45E-11	4.45E-11	8.91E-11	1.69E-08
Rockwell's 217F Predictions 50% Power De-rating and 50 °C case temperature, switching application and (2N5665 Theta_JC = 3.3 °C/W; 2N5038 Theta_JC = 1.3 °C/W) Environment = Space Flight	2.26E-10	1.39E-09	1.62E-09	3.07E-07
Similar to Rockwell's 217F Predictions except that (2N5665 Theta_JC = 2.6 C/W; 2N5038 Theta_JC = 1.3 C/W)	1.92E-10	1.39E-09	1.58E-09	3.00E-07
Similar to Rockwell's 217F Predictions except that application is linear (2N5665 Theta_JC = 3.3 C/W; 2N5038 Theta_JC = 1.3 C/W)	4.85E-10	2.98E-09	3.46E-09	6.58E-07
Similar to Rockwell's 217F Predictions except that application is linear (2N5665 Theta_JC = 2.6 C/W; 2N5038 Theta_JC = 1.3 C/W)	4.12E-10	2.98E-09	3.39E-09	6.44E-07
217C Predictions 50% Power De-rating, linear application	2.07E-09	8.06E-09	1.01E-08	1.93E-06
217C Predictions 50% De-rating, switching application	9.66E-10	3.76E-09	4.73E-09	8.98E-07

SAIC [1] used the PRISM software and predicted a failure rate of 18.8E-9 per hour for each transistor and a failure rate of 37.7E-9 per hour for a pair of transistors. They did not describe the assumptions for the PRISM failure rate predictions. The single prediction

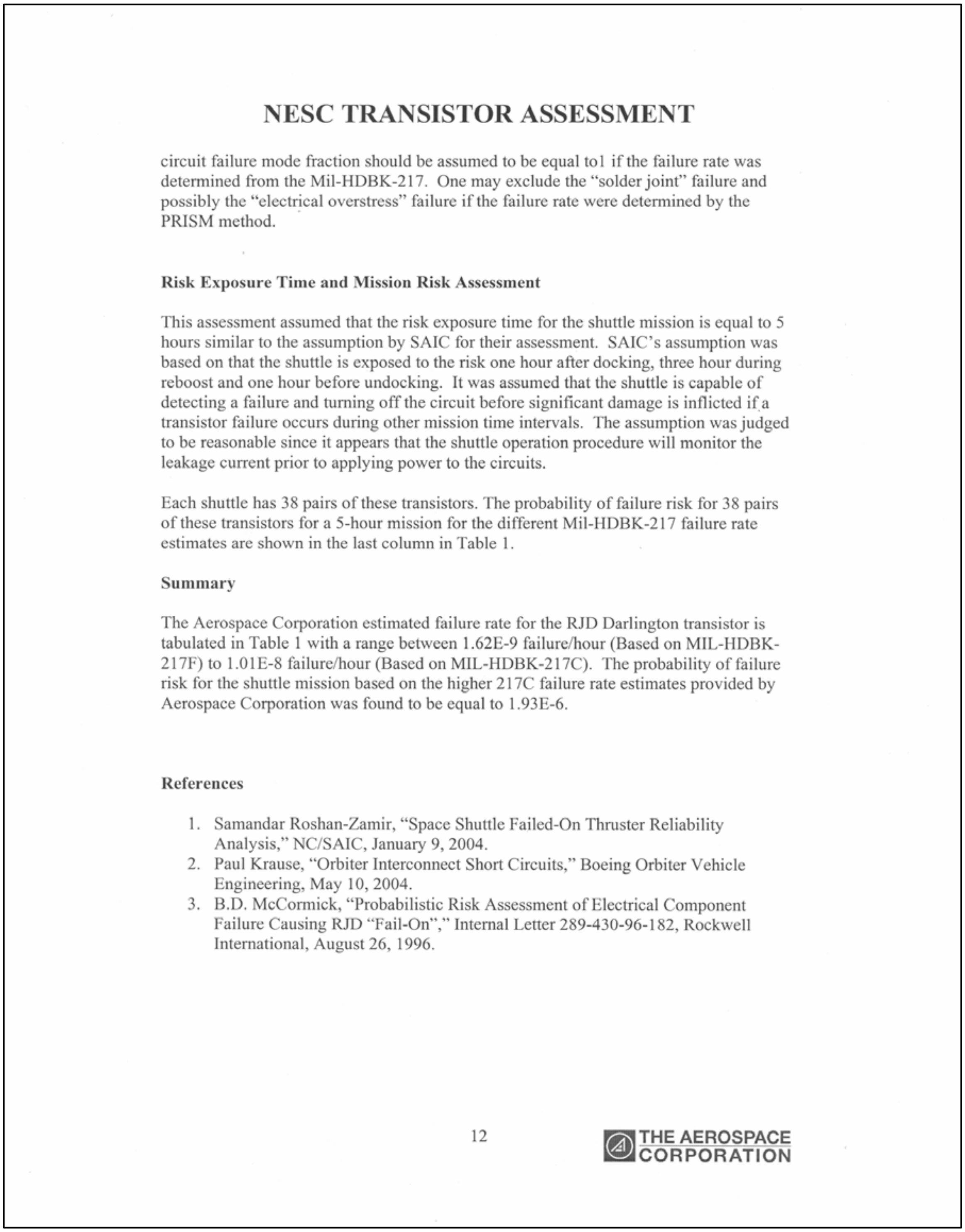


suggests that SAIC did not consider that the transistors were different. Their failure rate prediction was higher than the 217F predictions shown in Table 1. One possible reason for the much higher failure rate predictions was that SAIC might have used the PRISM RAC Rate Model and assumed that the transistors were manufactured long time ago. PRISM's RAC Rate Model includes a feature to apply a scale factor for adjusting the predicted failure rate based on the part vintage. The PRISM transistor predictions are very sensitive to the year of manufacture. For example, the so-called "operational" failure rate (after scaled by a 0.8 factor for the defaulted 80% duty cycle) for a switching NPN transistor (for a piece of communication equipment in the space flight environment) similar to the 2N5665 is predicted to be equal to 0.103E-9 failure/hour if it is manufactured in 2004, equal to 21.5E-9 failure/hour if it is manufactured in 1985 and equal to 87.8E-9 failure/hour if it is manufactured in 1980. The operational failure rate predictions for a switching NPN transistor similar to the 2N5038 for the corresponding vintages are equal to 0.332E-9, 69.2E-9 and 281.9E-9 failure/hour, respectively. These PRISM predictions illustrate the sensitivity of the prediction to the assumed part vintage and they should not be misconstrued to be the PRISM predictions for the two RJD transistors. PRISM provides the user many options to choose and modify the predictions. PRISM contains many RAC Rate Models for transistors and the models produce greatly different results. PRISM determines five separate failure rates ("operational", "non-operational", "cycling", "solder joint" and "electrical overstress") and calculates the total failure rate. SAIC failure rate prediction may or may not be the total failure rate. SAIC failure rate prediction provides no insight on the analysis except for that the predicted value is within the range of various Mil-HDBK-217 predictions. This assessment used the first set of failure rate predictions by Honeywell because it is more conservative than the others.

Transistor Short Circuit Failure Mode Fraction

SAIC assumed that the failure mode for a short between the Collector and the Emitter was the only critical failure mode. They assumed the 0.1% failure mode fraction based on a single number found in the RAC Failure Mode/Mechanism Distribution database (FMD-97). The 0.1% fraction was part of the 6.7% fraction assigned by RAC to an unclassified generic failure mode called "other." It is much smaller than the 48% "normalized" short circuit failure fraction for a NPN transistor reported by RAC. It is believed that the 0.1% fraction assumed by SAIC was incorrect because it was not supported by the RAC database and was not consistent with the circuit failure mode effects (e.g., a short between the Collector and the Base would activate the coil).

Except for a sudden wire bond failure, the initial failure mode for these two transistors was judged to be most likely experiencing excessive current leakage or short circuit of the junctions. Many short circuit failures often become an open circuit due to the subsequent excessive power dissipation. However, the failure mode for these two transistors is likely to remain being a short circuit or excessive current leakage because each thruster coil has 21.5-ohms D.C. resistance. The resistance will limit the maximum current (<2.6A) flow to be less than the rated Collector currents for the transistors (5 A and 20 A for 2N5665 and 2N5038, respectively). For risk assessment, the transistor short



NESC TRANSISTOR ASSESSMENT

circuit failure mode fraction should be assumed to be equal to1 if the failure rate was determined from the Mil-HDBK-217. One may exclude the “solder joint” failure and possibly the “electrical overstress” failure if the failure rate were determined by the PRISM method.

Risk Exposure Time and Mission Risk Assessment

This assessment assumed that the risk exposure time for the shuttle mission is equal to 5 hours similar to the assumption by SAIC for their assessment. SAIC’s assumption was based on that the shuttle is exposed to the risk one hour after docking, three hour during reboost and one hour before undocking. It was assumed that the shuttle is capable of detecting a failure and turning off the circuit before significant damage is inflicted if a transistor failure occurs during other mission time intervals. The assumption was judged to be reasonable since it appears that the shuttle operation procedure will monitor the leakage current prior to applying power to the circuits.

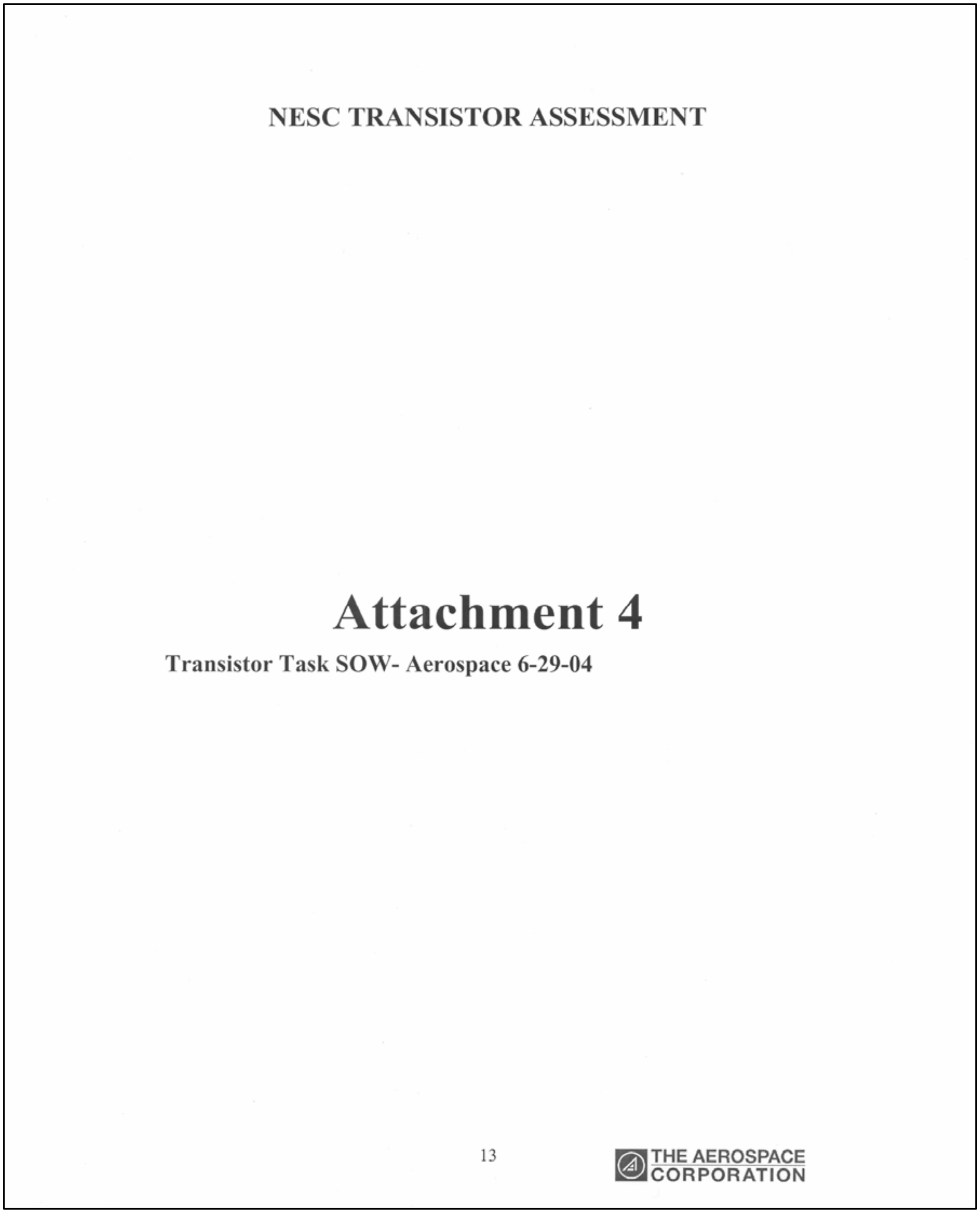
Each shuttle has 38 pairs of these transistors. The probability of failure risk for 38 pairs of these transistors for a 5-hour mission for the different Mil-HDBK-217 failure rate estimates are shown in the last column in Table 1.

Summary

The Aerospace Corporation estimated failure rate for the RJD Darlington transistor is tabulated in Table 1 with a range between 1.62E-9 failure/hour (Based on MIL-HDBK-217F) to 1.01E-8 failure/hour (Based on MIL-HDBK-217C). The probability of failure risk for the shuttle mission based on the higher 217C failure rate estimates provided by Aerospace Corporation was found to be equal to 1.93E-6.

References

1. Samandar Roshan-Zamir, “Space Shuttle Failed-On Thruster Reliability Analysis,” NC/SAIC, January 9, 2004.
2. Paul Krause, “Orbiter Interconnect Short Circuits,” Boeing Orbiter Vehicle Engineering, May 10, 2004.
3. B.D. McCormick, “Probabilistic Risk Assessment of Electrical Component Failure Causing RJD “Fail-On”,” Internal Letter 289-430-96-182, Rockwell International, August 26, 1996.

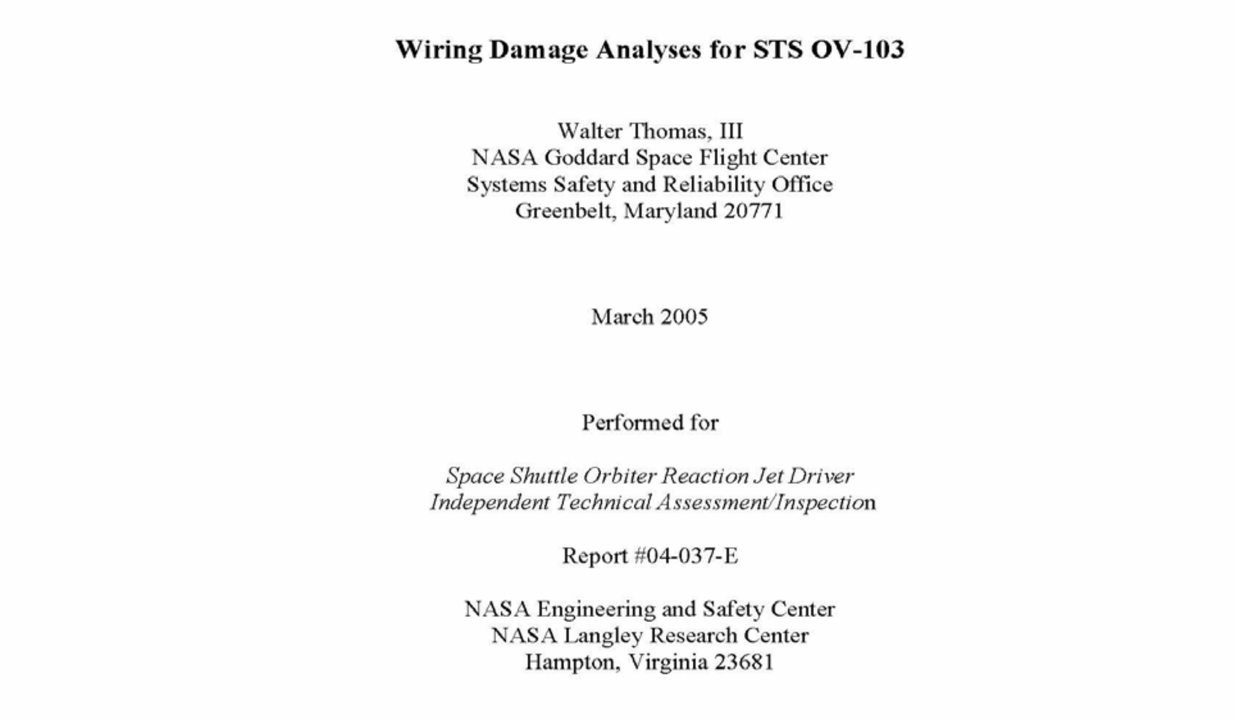


NESC TRANSISTOR ASSESSMENT

Attachment 4

Transistor Task SOW- Aerospace 6-29-04

Appendix G



Wiring Damage Analyses for STS OV-103

Walter Thomas, III
NASA Goddard Space Flight Center
Systems Safety and Reliability Office
Greenbelt, Maryland 20771

March 2005

Performed for

Space Shuttle Orbiter Reaction Jet Driver
Independent Technical Assessment/Inspection

Report #04-037-E

NASA Engineering and Safety Center
NASA Langley Research Center
Hampton, Virginia 23681

Contents

Acknowledgements iv

Executive Summary v

I. Introduction 1

II. Civil Aircraft Wiring Incidents 2

III. OV-103 Wiring Data – Initial Compilations 6

IV. The STS Wire Inspection/Maintenance Process and OV-103 Wiring Damage Events 12

V. OV-103 Wiring Damage by Failure Modes 17

VI. Discussion 23

VII. Conclusions and Recommendations 25

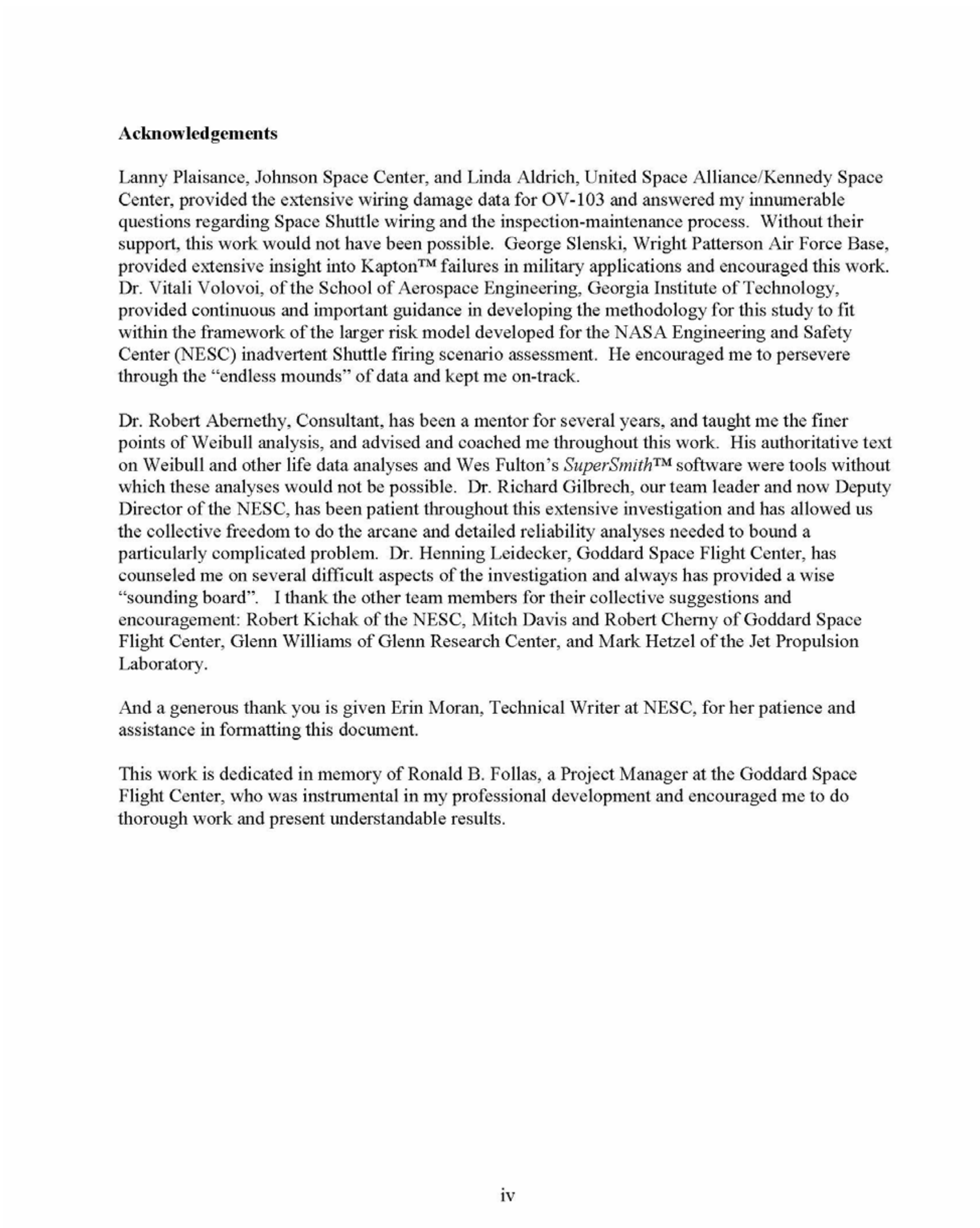
References 28

List of Tables

Table G-I Data compiled from FAA "AIDS" 2
Table G-II Numbers of wiring and wire shorting events for air carrier and commercial aircraft 4
Table G-III NESC Wiring Damage Codes 6
Table G-IV Summary Frequency Statistics OV-103 Wiring Damage Events 8
Table G-V OV-103 Wiring Damage Event Proportions 9
Table G-VI Normalized occurrence rates for OV-103 Wiring Damage Events 11
Table G-VII Summary of Weibull Parameters by Failure Mode 25

List of Figures

Figure G-1 Weibull Plot of Civil Aircraft Wiring Incidents 3
Figure G-2 Weibull plot of Air Carrier and Commercial Aircraft Wire Failure Incidents 5
Figure G-3 Weibull plots of Air Carrier and Commercial Aircraft Wiring Failure Incidents Separated by Failure Modes 5
Figure G-4 Pareto Chart for OV-103 Wiring Damage Events Over The Vehicle's Lifetime 10
Figure G-5 Crow-AMSAA Plot of STS Orbiter Interconnect Short Circuits 12
Figure G-6 Crow-AMSAA Plot of all OV-103 Wiring Damage Events 14
Figure G-7 Crow-AMSAA Plot of OV-103 *Detected* Wiring Damage Events by Vehicle Flight Number 15
Figure G-8 OV-103 Wiring Damage Events (By Flight Cycle) Plotted As Occurrence Rates, from CA Plot 16
Figure G-9 Weibull Plot of OV-103 Wiring Short-Circuit Events 18
Figure G-10 Weibull Plot of Kaplan-Meier Data for OV-103 Exposed Conductor Events 19
Figure G-11 Weibull Plot (K-M) for OV-103 Kapton™ cracking and Ring Cracks 20
Figure G-12 Weibull Plot of Other Kapton™ Damage Events (KD and KS) 21
Figure G-13 Weibull (K-M) Plot of wire Chaffing Events 22
Figure G-14 Weibull (K-M) Plot of Broken Wire Events 22



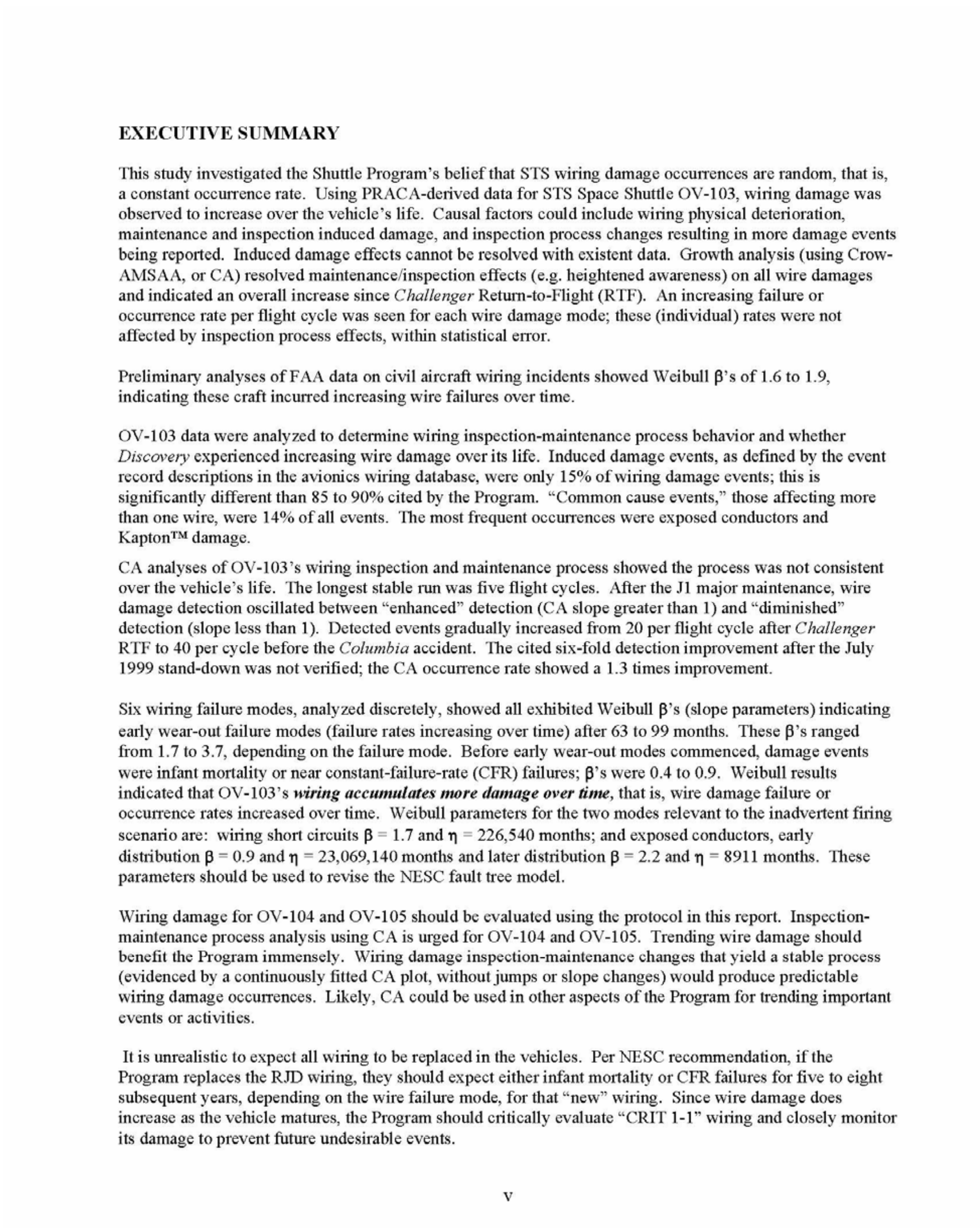
Acknowledgements

Lanny Plaisance, Johnson Space Center, and Linda Aldrich, United Space Alliance/Kennedy Space Center, provided the extensive wiring damage data for OV-103 and answered my innumerable questions regarding Space Shuttle wiring and the inspection-maintenance process. Without their support, this work would not have been possible. George Slenski, Wright Patterson Air Force Base, provided extensive insight into Kapton™ failures in military applications and encouraged this work. Dr. Vitali Volovoi, of the School of Aerospace Engineering, Georgia Institute of Technology, provided continuous and important guidance in developing the methodology for this study to fit within the framework of the larger risk model developed for the NASA Engineering and Safety Center (NESC) inadvertent Shuttle firing scenario assessment. He encouraged me to persevere through the "endless mounds" of data and kept me on-track.

Dr. Robert Abernethy, Consultant, has been a mentor for several years, and taught me the finer points of Weibull analysis, and advised and coached me throughout this work. His authoritative text on Weibull and other life data analyses and Wes Fulton's *SuperSmith*™ software were tools without which these analyses would not be possible. Dr. Richard Gilbrech, our team leader and now Deputy Director of the NESC, has been patient throughout this extensive investigation and has allowed us the collective freedom to do the arcane and detailed reliability analyses needed to bound a particularly complicated problem. Dr. Henning Leidecker, Goddard Space Flight Center, has counseled me on several difficult aspects of the investigation and always has provided a wise "sounding board". I thank the other team members for their collective suggestions and encouragement: Robert Kichak of the NESC, Mitch Davis and Robert Cherny of Goddard Space Flight Center, Glenn Williams of Glenn Research Center, and Mark Hetzel of the Jet Propulsion Laboratory.

And a generous thank you is given Erin Moran, Technical Writer at NESC, for her patience and assistance in formatting this document.

This work is dedicated in memory of Ronald B. Follas, a Project Manager at the Goddard Space Flight Center, who was instrumental in my professional development and encouraged me to do thorough work and present understandable results.



EXECUTIVE SUMMARY

This study investigated the Shuttle Program's belief that STS wiring damage occurrences are random, that is, a constant occurrence rate. Using PRACA-derived data for STS Space Shuttle OV-103, wiring damage was observed to increase over the vehicle's life. Causal factors could include wiring physical deterioration, maintenance and inspection induced damage, and inspection process changes resulting in more damage events being reported. Induced damage effects cannot be resolved with existent data. Growth analysis (using Crow-AMSAA, or CA) resolved maintenance/inspection effects (e.g. heightened awareness) on all wire damages and indicated an overall increase since *Challenger* Return-to-Flight (RTF). An increasing failure or occurrence rate per flight cycle was seen for each wire damage mode; these (individual) rates were not affected by inspection process effects, within statistical error.

Preliminary analyses of FAA data on civil aircraft wiring incidents showed Weibull β's of 1.6 to 1.9, indicating these craft incurred increasing wire failures over time.

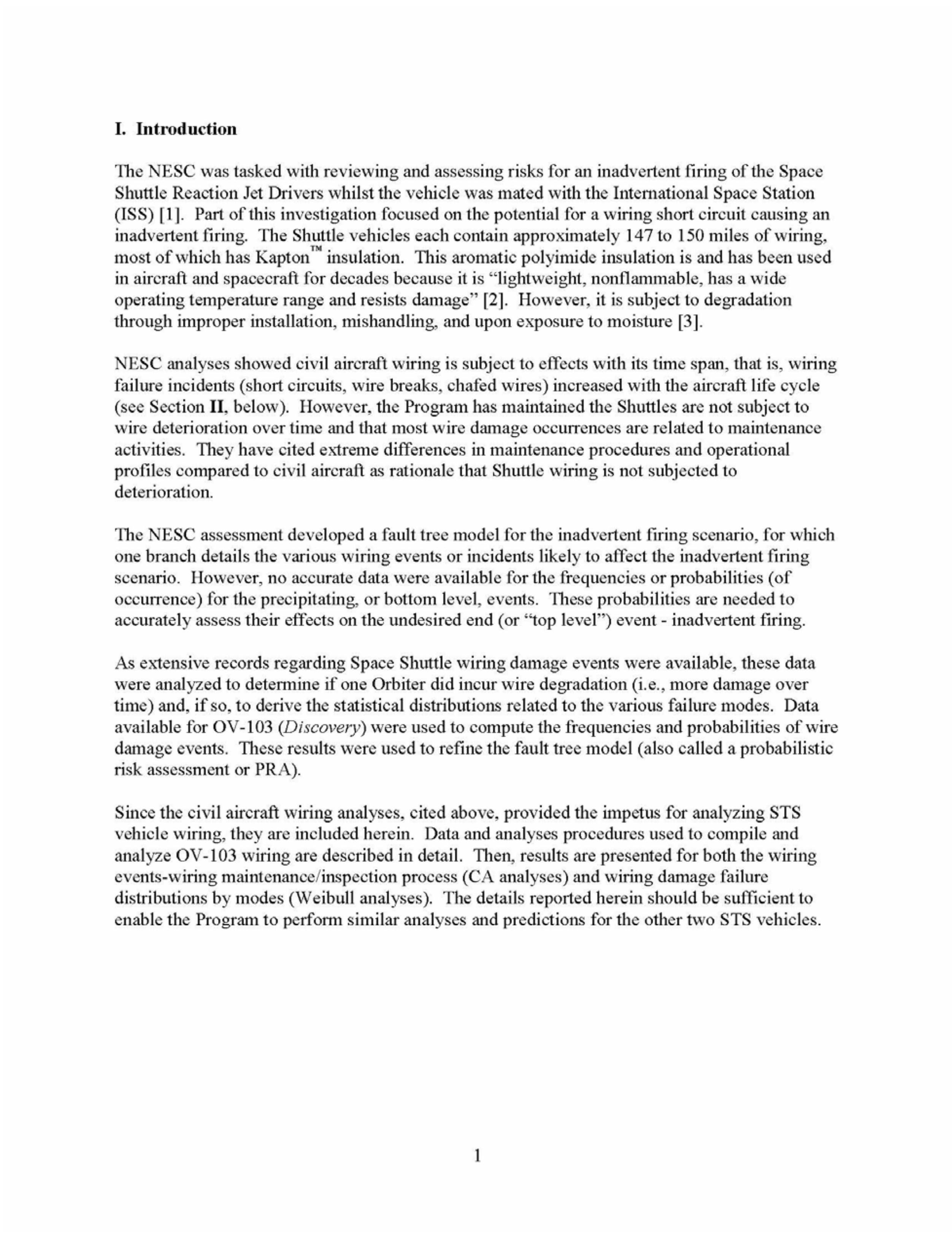
OV-103 data were analyzed to determine wiring inspection-maintenance process behavior and whether *Discovery* experienced increasing wire damage over its life. Induced damage events, as defined by the event record descriptions in the avionics wiring database, were only 15% of wiring damage events; this is significantly different than 85 to 90% cited by the Program. "Common cause events," those affecting more than one wire, were 14% of all events. The most frequent occurrences were exposed conductors and Kapton™ damage.

CA analyses of OV-103's wiring inspection and maintenance process showed the process was not consistent over the vehicle's life. The longest stable run was five flight cycles. After the J1 major maintenance, wire damage detection oscillated between "enhanced" detection (CA slope greater than 1) and "diminished" detection (slope less than 1). Detected events gradually increased from 20 per flight cycle after *Challenger* RTF to 40 per cycle before the *Columbia* accident. The cited six-fold detection improvement after the July 1999 stand-down was not verified; the CA occurrence rate showed a 1.3 times improvement.

Six wiring failure modes, analyzed discretely, showed all exhibited Weibull β's (slope parameters) indicating early wear-out failure modes (failure rates increasing over time) after 63 to 99 months. These β's ranged from 1.7 to 3.7, depending on the failure mode. Before early wear-out modes commenced, damage events were infant mortality or near constant-failure-rate (CFR) failures; β's were 0.4 to 0.9. Weibull results indicated that OV-103's ***wiring accumulates more damage over time***, that is, wire damage failure or occurrence rates increased over time. Weibull parameters for the two modes relevant to the inadvertent firing scenario are: wiring short circuits $\beta = 1.7$ and $\eta = 226{,}540$ months; and exposed conductors, early distribution $\beta = 0.9$ and $\eta = 23{,}069{,}140$ months and later distribution $\beta = 2.2$ and $\eta = 8911$ months. These parameters should be used to revise the NESC fault tree model.

Wiring damage for OV-104 and OV-105 should be evaluated using the protocol in this report. Inspection-maintenance process analysis using CA is urged for OV-104 and OV-105. Trending wire damage should benefit the Program immensely. Wiring damage inspection-maintenance changes that yield a stable process (evidenced by a continuously fitted CA plot, without jumps or slope changes) would produce predictable wiring damage occurrences. Likely, CA could be used in other aspects of the Program for trending important events or activities.

It is unrealistic to expect all wiring to be replaced in the vehicles. Per NESC recommendation, if the Program replaces the RJD wiring, they should expect either infant mortality or CFR failures for five to eight subsequent years, depending on the wire failure mode, for that "new" wiring. Since wire damage does increase as the vehicle matures, the Program should critically evaluate "CRIT 1-1" wiring and closely monitor its damage to prevent future undesirable events.



I. Introduction

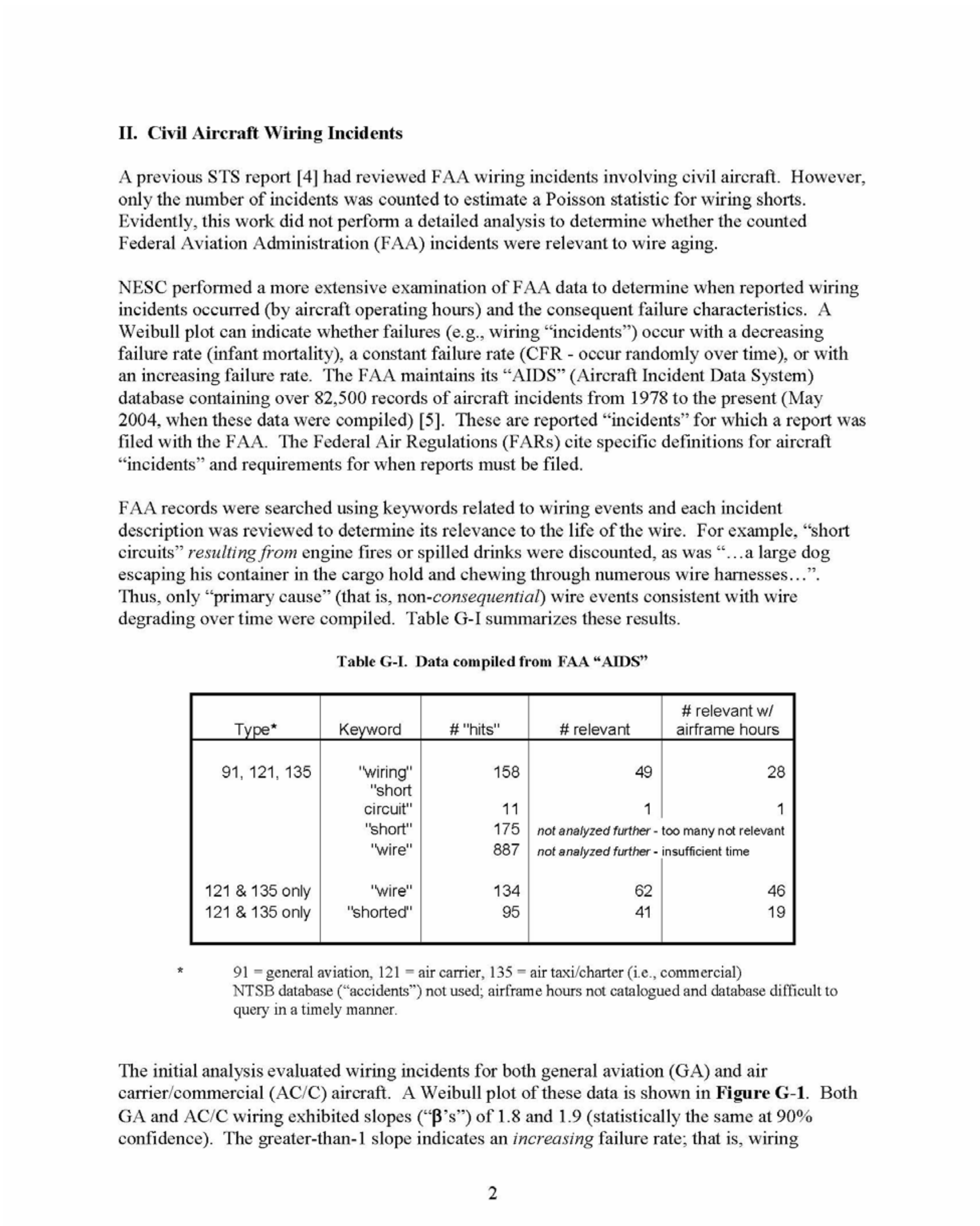
The NESC was tasked with reviewing and assessing risks for an inadvertent firing of the Space Shuttle Reaction Jet Drivers whilst the vehicle was mated with the International Space Station (ISS) [1]. Part of this investigation focused on the potential for a wiring short circuit causing an inadvertent firing. The Shuttle vehicles each contain approximately 147 to 150 miles of wiring, most of which has Kapton™ insulation. This aromatic polyimide insulation is and has been used in aircraft and spacecraft for decades because it is "lightweight, nonflammable, has a wide operating temperature range and resists damage" [2]. However, it is subject to degradation through improper installation, mishandling, and upon exposure to moisture [3].

NESC analyses showed civil aircraft wiring is subject to effects with its time span, that is, wiring failure incidents (short circuits, wire breaks, chafed wires) increased with the aircraft life cycle (see Section **II**, below). However, the Program has maintained the Shuttles are not subject to wire deterioration over time and that most wire damage occurrences are related to maintenance activities. They have cited extreme differences in maintenance procedures and operational profiles compared to civil aircraft as rationale that Shuttle wiring is not subjected to deterioration.

The NESC assessment developed a fault tree model for the inadvertent firing scenario, for which one branch details the various wiring events or incidents likely to affect the inadvertent firing scenario. However, no accurate data were available for the frequencies or probabilities (of occurrence) for the precipitating, or bottom level, events. These probabilities are needed to accurately assess their effects on the undesired end (or "top level") event - inadvertent firing.

As extensive records regarding Space Shuttle wiring damage events were available, these data were analyzed to determine if one Orbiter did incur wire degradation (i.e., more damage over time) and, if so, to derive the statistical distributions related to the various failure modes. Data available for OV-103 (*Discovery*) were used to compute the frequencies and probabilities of wire damage events. These results were used to refine the fault tree model (also called a probabilistic risk assessment or PRA).

Since the civil aircraft wiring analyses, cited above, provided the impetus for analyzing STS vehicle wiring, they are included herein. Data and analyses procedures used to compile and analyze OV-103 wiring are described in detail. Then, results are presented for both the wiring events-wiring maintenance/inspection process (CA analyses) and wiring damage failure distributions by modes (Weibull analyses). The details reported herein should be sufficient to enable the Program to perform similar analyses and predictions for the other two STS vehicles.



II. Civil Aircraft Wiring Incidents

A previous STS report [4] had reviewed FAA wiring incidents involving civil aircraft. However, only the number of incidents was counted to estimate a Poisson statistic for wiring shorts. Evidently, this work did not perform a detailed analysis to determine whether the counted Federal Aviation Administration (FAA) incidents were relevant to wire aging.

NESC performed a more extensive examination of FAA data to determine when reported wiring incidents occurred (by aircraft operating hours) and the consequent failure characteristics. A Weibull plot can indicate whether failures (e.g., wiring "incidents") occur with a decreasing failure rate (infant mortality), a constant failure rate (CFR - occur randomly over time), or with an increasing failure rate. The FAA maintains its "AIDS" (Aircraft Incident Data System) database containing over 82,500 records of aircraft incidents from 1978 to the present (May 2004, when these data were compiled) [5]. These are reported "incidents" for which a report was filed with the FAA. The Federal Air Regulations (FARs) cite specific definitions for aircraft "incidents" and requirements for when reports must be filed.

FAA records were searched using keywords related to wiring events and each incident description was reviewed to determine its relevance to the life of the wire. For example, "short circuits" *resulting from* engine fires or spilled drinks were discounted, as was "…a large dog escaping his container in the cargo hold and chewing through numerous wire harnesses…". Thus, only "primary cause" (that is, non-*consequential*) wire events consistent with wire degrading over time were compiled. Table G-I summarizes these results.

Table G-I. Data compiled from FAA "AIDS"

Type*	Keyword	# "hits"	# relevant	# relevant w/ airframe hours
91, 121, 135	"wiring"	158	49	28
	"short circuit"	11	1	1
	"short"	175	*not analyzed further* - too many not relevant	
	"wire"	887	*not analyzed further* - insufficient time	
121 & 135 only	"wire"	134	62	46
121 & 135 only	"shorted"	95	41	19

* 91 = general aviation, 121 = air carrier, 135 = air taxi/charter (i.e., commercial)
NTSB database ("accidents") not used; airframe hours not catalogued and database difficult to query in a timely manner.

The initial analysis evaluated wiring incidents for both general aviation (GA) and air carrier/commercial (AC/C) aircraft. A Weibull plot of these data is shown in **Figure G-1**. Both GA and AC/C wiring exhibited slopes ("**β**'s") of 1.8 and 1.9 (statistically the same at 90% confidence). The greater-than-1 slope indicates an *increasing* failure rate; that is, wiring incidents are occurring more frequently as aircraft accumulate operating hours. The identical slopes imply failures occurred with similar modes (failure mechanisms). Characteristics lives (“**η**”) were 9020 and 31,200 airframe hours, respectively. The behavior of characteristic lives is very interesting. Generally, AC/C aircraft accrue considerably more operating hours per calendar year than GA aircraft. Thus, one would expect the AC/C failure distribution to coincide or precede that for GA aircraft. However, the AC/C plot is displaced approximately 20,000 hours *later*. This suggests a causal factor other than aircraft operating hours, when GA and AC/C are compared. (No data were available for aircraft calendar ages at the event times). Nonetheless, these data do show that civil aircraft wiring incidents exhibit an increasing failure rate with time.

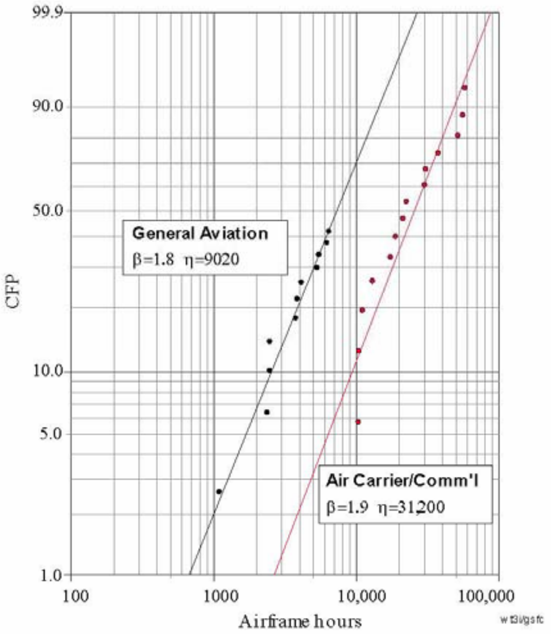


Figure G-1. Weibull plot of civil aircraft wiring “incidents”. Data for both GA and AC/C aircraft have the same slope, but are displaced along the time axis.

Subsequent analyses of the FAA data focused on air carrier and commercial operations only. Additional data were compiled, producing the following numbers of relevant wiring incidents for AC/C aircraft:

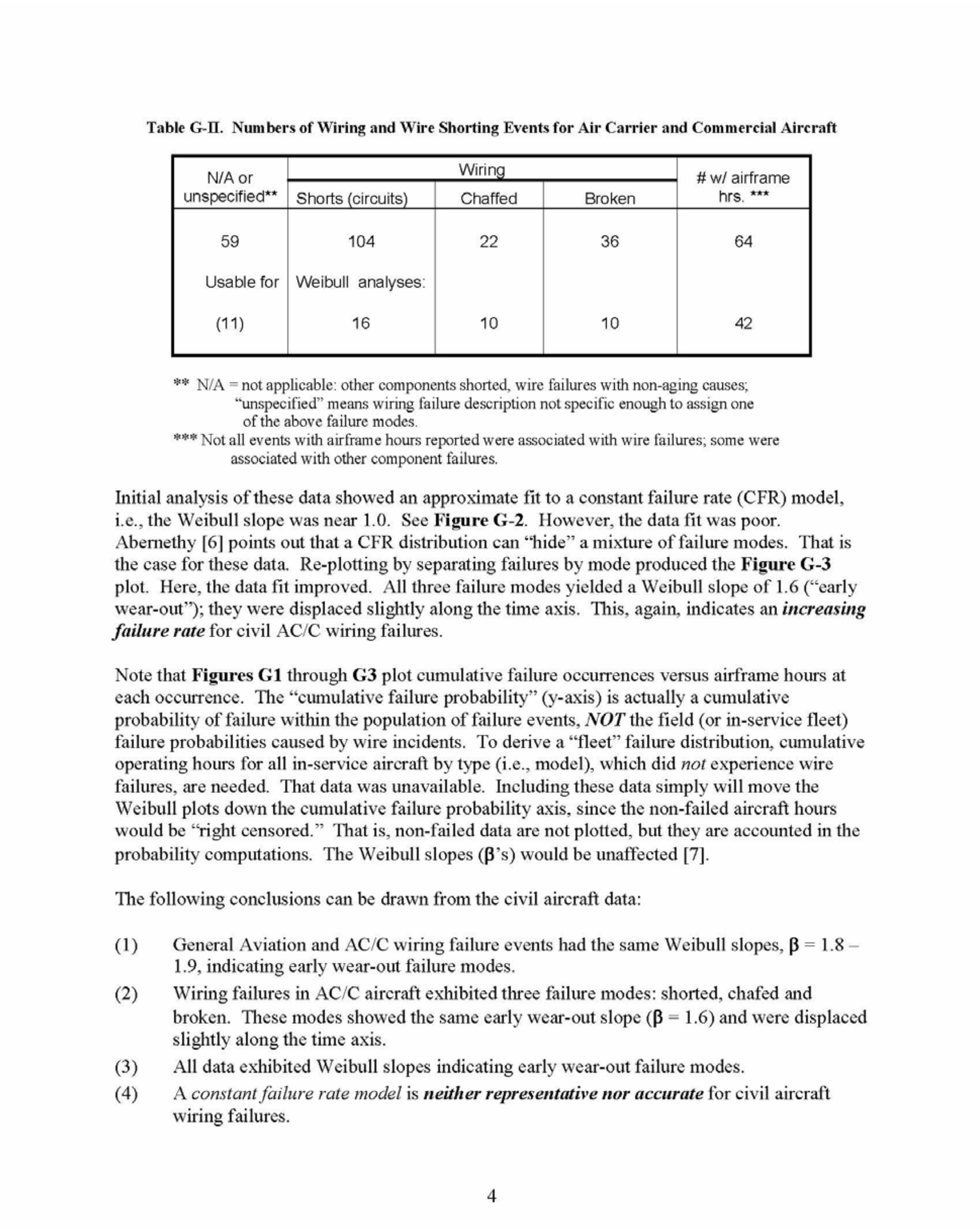


Table G-II. Numbers of Wiring and Wire Shorting Events for Air Carrier and Commercial Aircraft

N/A or unspecified**	Wiring			# w/ airframe hrs. ***
	Shorts (circuits)	Chaffed	Broken	
59	104	22	36	64
Usable for	Weibull analyses:			
(11)	16	10	10	42

** N/A = not applicable: other components shorted, wire failures with non-aging causes; "unspecified" means wiring failure description not specific enough to assign one of the above failure modes.

*** Not all events with airframe hours reported were associated with wire failures; some were associated with other component failures.

Initial analysis of these data showed an approximate fit to a constant failure rate (CFR) model, i.e., the Weibull slope was near 1.0. See **Figure G-2**. However, the data fit was poor. Abernethy [6] points out that a CFR distribution can "hide" a mixture of failure modes. That is the case for these data. Re-plotting by separating failures by mode produced the **Figure G-3** plot. Here, the data fit improved. All three failure modes yielded a Weibull slope of 1.6 ("early wear-out"); they were displaced slightly along the time axis. This, again, indicates an ***increasing failure rate*** for civil AC/C wiring failures.

Note that **Figures G1** through **G3** plot cumulative failure occurrences versus airframe hours at each occurrence. The "cumulative failure probability" (y-axis) is actually a cumulative probability of failure within the population of failure events, ***NOT*** the field (or in-service fleet) failure probabilities caused by wire incidents. To derive a "fleet" failure distribution, cumulative operating hours for all in-service aircraft by type (i.e., model), which did *not* experience wire failures, are needed. That data was unavailable. Including these data simply will move the Weibull plots down the cumulative failure probability axis, since the non-failed aircraft hours would be "right censored." That is, non-failed data are not plotted, but they are accounted in the probability computations. The Weibull slopes (**β**'s) would be unaffected [7].

The following conclusions can be drawn from the civil aircraft data:

(1) General Aviation and AC/C wiring failure events had the same Weibull slopes, **β** = 1.8 – 1.9, indicating early wear-out failure modes.

(2) Wiring failures in AC/C aircraft exhibited three failure modes: shorted, chafed and broken. These modes showed the same early wear-out slope (**β** = 1.6) and were displaced slightly along the time axis.

(3) All data exhibited Weibull slopes indicating early wear-out failure modes.

(4) A *constant failure rate model* is ***neither representative nor accurate*** for civil aircraft wiring failures.

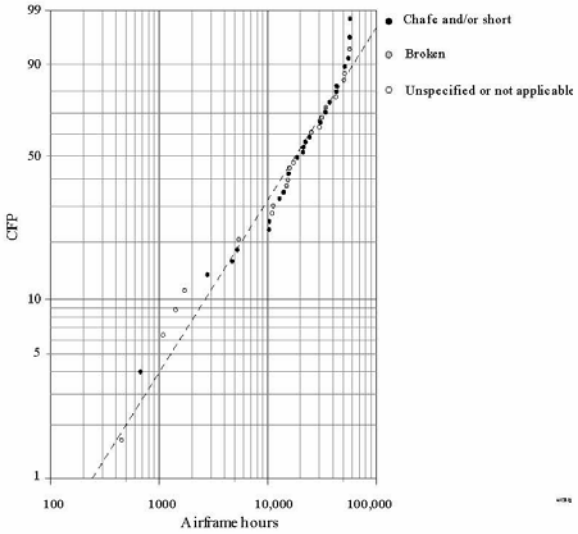


Figure G-2. Weibull plot of Air Carrier and Commercial aircraft wire failure incidents. Apparent Weibull slope (β – the dashed line) is ~ 1, but data clearly indicates mixture of failure modes (plot is not linear). Failures are coded according to legend in upper right.

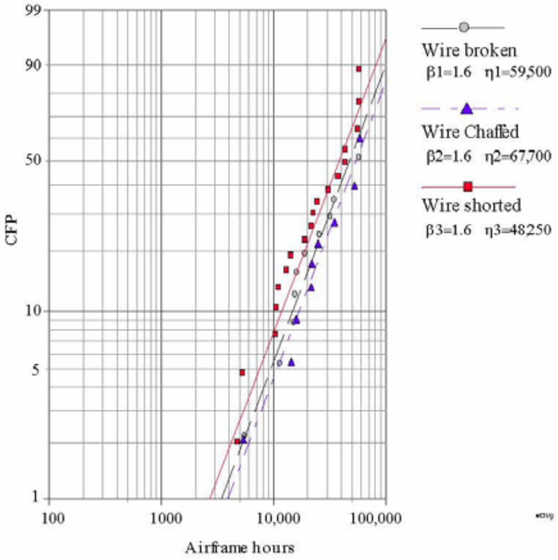
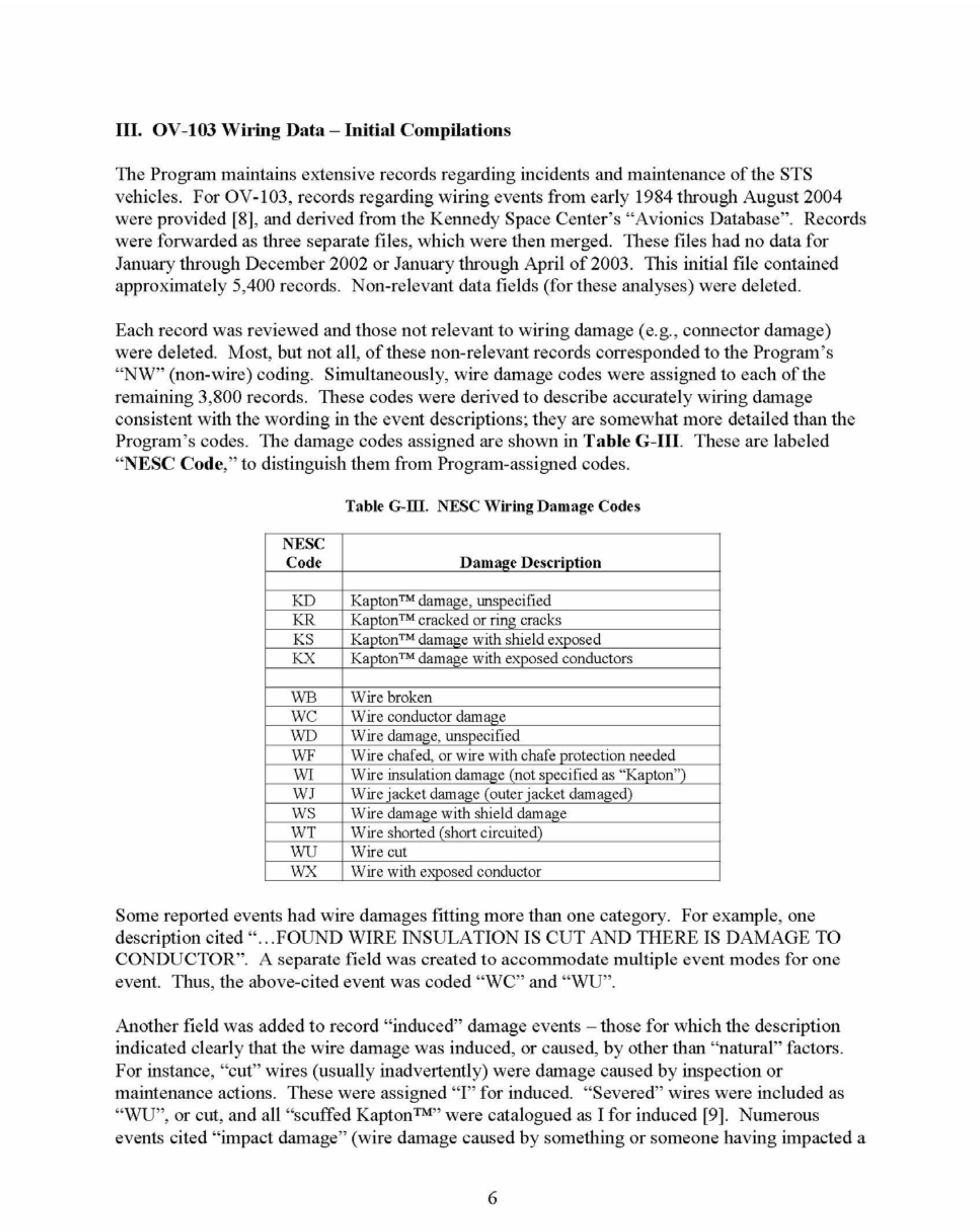


Figure G-3. Weibull plots of Air Carrier and Commercial Operations wiring failure incidents separated by failure modes. The three modes have the same Weibull slopes and are displaced slightly along the time axis. Wiring failures are *not consistent* with a constant failure rate model.



III. OV-103 Wiring Data – Initial Compilations

The Program maintains extensive records regarding incidents and maintenance of the STS vehicles. For OV-103, records regarding wiring events from early 1984 through August 2004 were provided [8], and derived from the Kennedy Space Center's "Avionics Database". Records were forwarded as three separate files, which were then merged. These files had no data for January through December 2002 or January through April of 2003. This initial file contained approximately 5,400 records. Non-relevant data fields (for these analyses) were deleted.

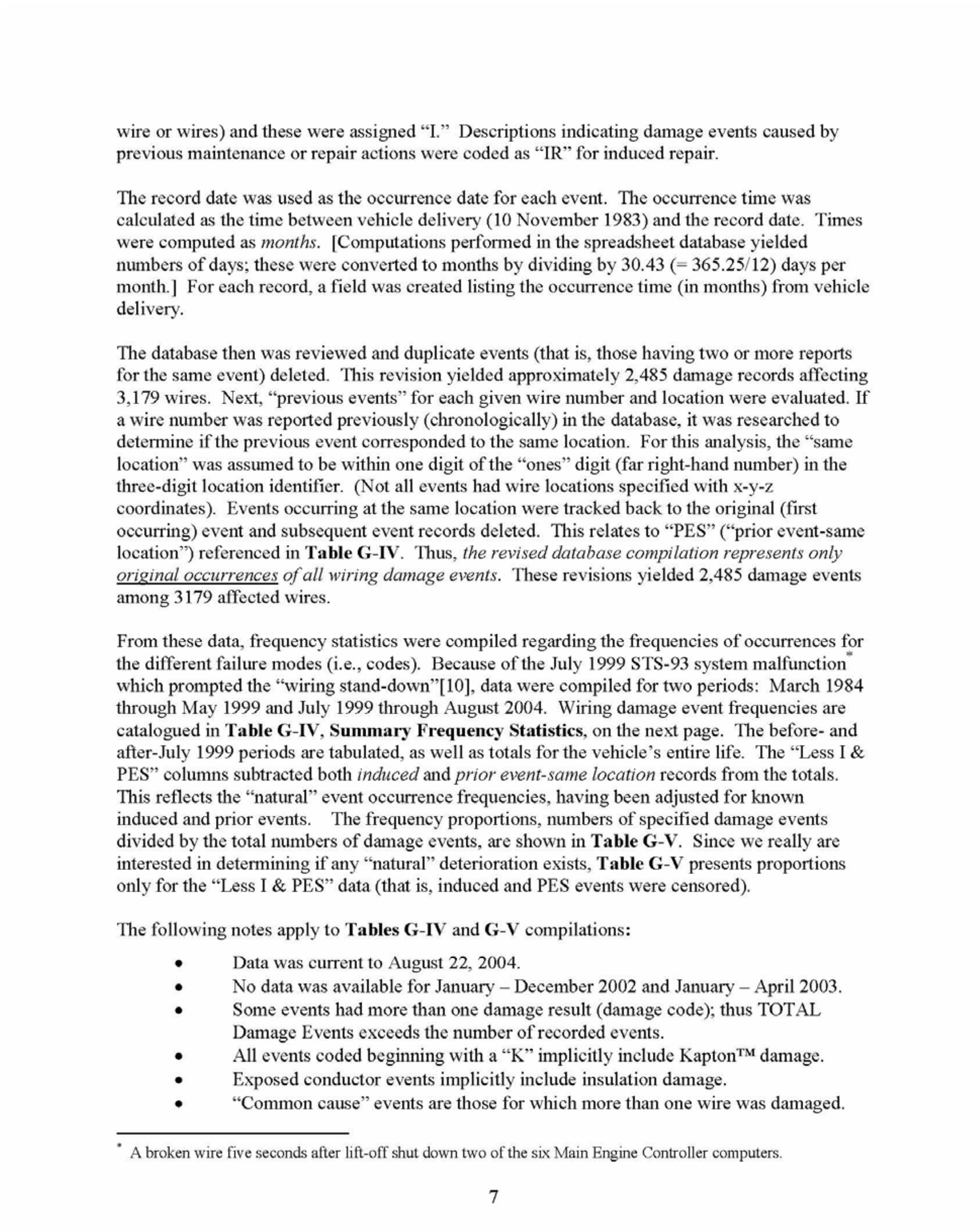
Each record was reviewed and those not relevant to wiring damage (e.g., connector damage) were deleted. Most, but not all, of these non-relevant records corresponded to the Program's "NW" (non-wire) coding. Simultaneously, wire damage codes were assigned to each of the remaining 3,800 records. These codes were derived to describe accurately wiring damage consistent with the wording in the event descriptions; they are somewhat more detailed than the Program's codes. The damage codes assigned are shown in **Table G-III**. These are labeled "**NESC Code**," to distinguish them from Program-assigned codes.

Table G-III. NESC Wiring Damage Codes

NESC Code	Damage Description
KD	Kapton™ damage, unspecified
KR	Kapton™ cracked or ring cracks
KS	Kapton™ damage with shield exposed
KX	Kapton™ damage with exposed conductors
WB	Wire broken
WC	Wire conductor damage
WD	Wire damage, unspecified
WF	Wire chafed, or wire with chafe protection needed
WI	Wire insulation damage (not specified as "Kapton")
WJ	Wire jacket damage (outer jacket damaged)
WS	Wire damage with shield damage
WT	Wire shorted (short circuited)
WU	Wire cut
WX	Wire with exposed conductor

Some reported events had wire damages fitting more than one category. For example, one description cited "…FOUND WIRE INSULATION IS CUT AND THERE IS DAMAGE TO CONDUCTOR". A separate field was created to accommodate multiple event modes for one event. Thus, the above-cited event was coded "WC" and "WU".

Another field was added to record "induced" damage events – those for which the description indicated clearly that the wire damage was induced, or caused, by other than "natural" factors. For instance, "cut" wires (usually inadvertently) were damage caused by inspection or maintenance actions. These were assigned "I" for induced. "Severed" wires were included as "WU", or cut, and all "scuffed Kapton™" were catalogued as I for induced [9]. Numerous events cited "impact damage" (wire damage caused by something or someone having impacted a



wire or wires) and these were assigned "I." Descriptions indicating damage events caused by previous maintenance or repair actions were coded as "IR" for induced repair.

The record date was used as the occurrence date for each event. The occurrence time was calculated as the time between vehicle delivery (10 November 1983) and the record date. Times were computed as *months*. [Computations performed in the spreadsheet database yielded numbers of days; these were converted to months by dividing by 30.43 (= 365.25/12) days per month.] For each record, a field was created listing the occurrence time (in months) from vehicle delivery.

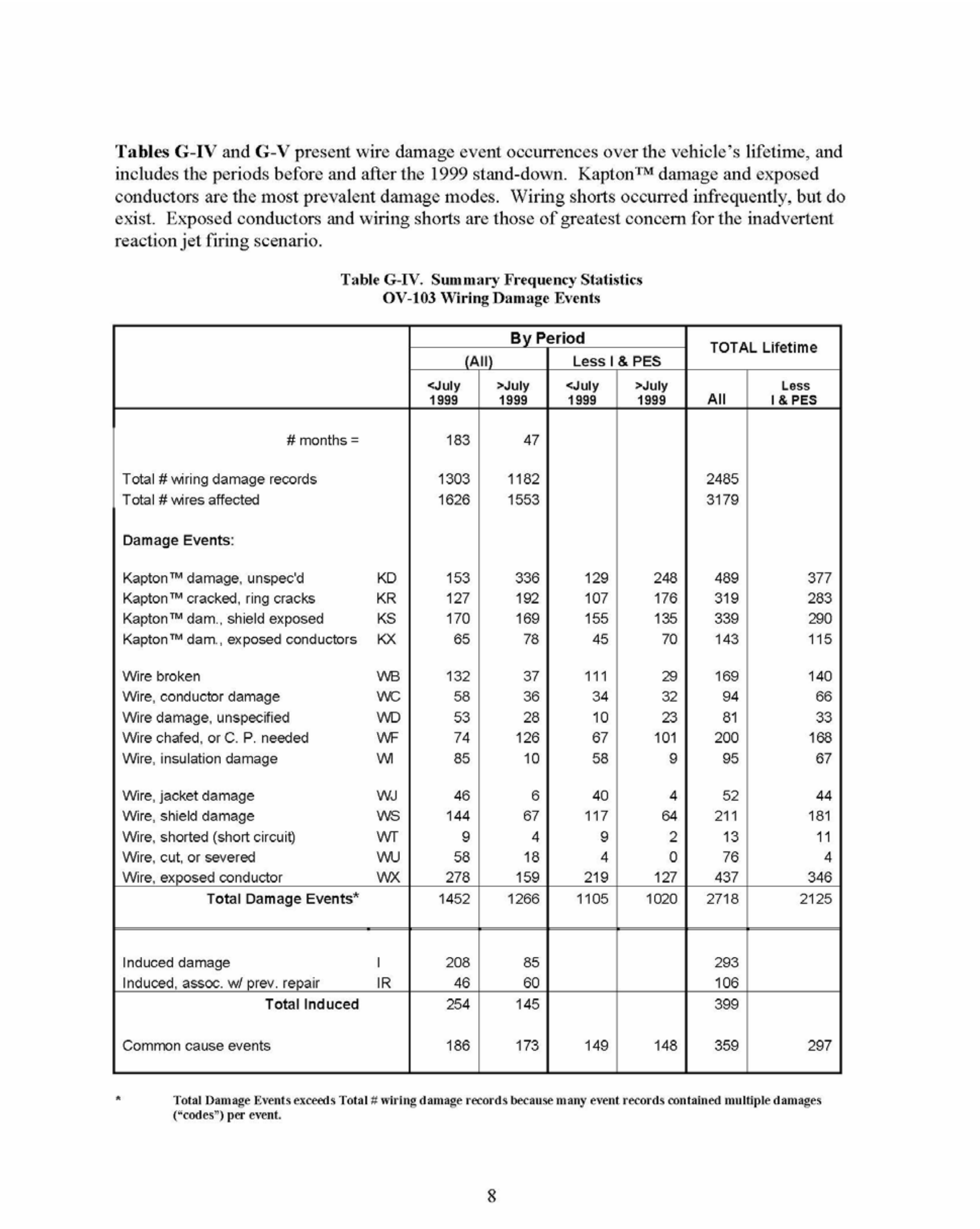
The database then was reviewed and duplicate events (that is, those having two or more reports for the same event) deleted. This revision yielded approximately 2,485 damage records affecting 3,179 wires. Next, "previous events" for each given wire number and location were evaluated. If a wire number was reported previously (chronologically) in the database, it was researched to determine if the previous event corresponded to the same location. For this analysis, the "same location" was assumed to be within one digit of the "ones" digit (far right-hand number) in the three-digit location identifier. (Not all events had wire locations specified with x-y-z coordinates). Events occurring at the same location were tracked back to the original (first occurring) event and subsequent event records deleted. This relates to "PES" ("prior event-same location") referenced in **Table G-IV**. Thus, *the revised database compilation represents only original occurrences of all wiring damage events*. These revisions yielded 2,485 damage events among 3179 affected wires.

From these data, frequency statistics were compiled regarding the frequencies of occurrences for the different failure modes (i.e., codes). Because of the July 1999 STS-93 system malfunction* which prompted the "wiring stand-down"[10], data were compiled for two periods: March 1984 through May 1999 and July 1999 through August 2004. Wiring damage event frequencies are catalogued in **Table G-IV**, **Summary Frequency Statistics**, on the next page. The before- and after-July 1999 periods are tabulated, as well as totals for the vehicle's entire life. The "Less I & PES" columns subtracted both *induced* and *prior event-same location* records from the totals. This reflects the "natural" event occurrence frequencies, having been adjusted for known induced and prior events. The frequency proportions, numbers of specified damage events divided by the total numbers of damage events, are shown in **Table G-V**. Since we really are interested in determining if any "natural" deterioration exists, **Table G-V** presents proportions only for the "Less I & PES" data (that is, induced and PES events were censored).

The following notes apply to **Tables G-IV** and **G-V** compilations:

- Data was current to August 22, 2004.
- No data was available for January – December 2002 and January – April 2003.
- Some events had more than one damage result (damage code); thus TOTAL Damage Events exceeds the number of recorded events.
- All events coded beginning with a "K" implicitly include Kapton™ damage.
- Exposed conductor events implicitly include insulation damage.
- "Common cause" events are those for which more than one wire was damaged.

* A broken wire five seconds after lift-off shut down two of the six Main Engine Controller computers.



Tables G-IV and **G-V** present wire damage event occurrences over the vehicle's lifetime, and includes the periods before and after the 1999 stand-down. Kapton™ damage and exposed conductors are the most prevalent damage modes. Wiring shorts occurred infrequently, but do exist. Exposed conductors and wiring shorts are those of greatest concern for the inadvertent reaction jet firing scenario.

Table G-IV. Summary Frequency Statistics
OV-103 Wiring Damage Events

		By Period				TOTAL Lifetime	
		(All)		Less I & PES			
		<July 1999	>July 1999	<July 1999	>July 1999	All	Less I & PES
# months =		183	47				
Total # wiring damage records		1303	1182			2485	
Total # wires affected		1626	1553			3179	
Damage Events:							
Kapton™ damage, unspec'd	KD	153	336	129	248	489	377
Kapton™ cracked, ring cracks	KR	127	192	107	176	319	283
Kapton™ dam., shield exposed	KS	170	169	155	135	339	290
Kapton™ dam., exposed conductors	KX	65	78	45	70	143	115
Wire broken	WB	132	37	111	29	169	140
Wire, conductor damage	WC	58	36	34	32	94	66
Wire damage, unspecified	WD	53	28	10	23	81	33
Wire chafed, or C. P. needed	WF	74	126	67	101	200	168
Wire, insulation damage	WI	85	10	58	9	95	67
Wire, jacket damage	WJ	46	6	40	4	52	44
Wire, shield damage	WS	144	67	117	64	211	181
Wire, shorted (short circuit)	WT	9	4	9	2	13	11
Wire, cut, or severed	WU	58	18	4	0	76	4
Wire, exposed conductor	WX	278	159	219	127	437	346
Total Damage Events*		1452	1266	1105	1020	2718	2125
Induced damage	I	208	85			293	
Induced, assoc. w/ prev. repair	IR	46	60			106	
Total Induced		254	145			399	
Common cause events		186	173	149	148	359	297

* **Total Damage Events exceeds Total # wiring damage records because many event records contained multiple damages ("codes") per event.**

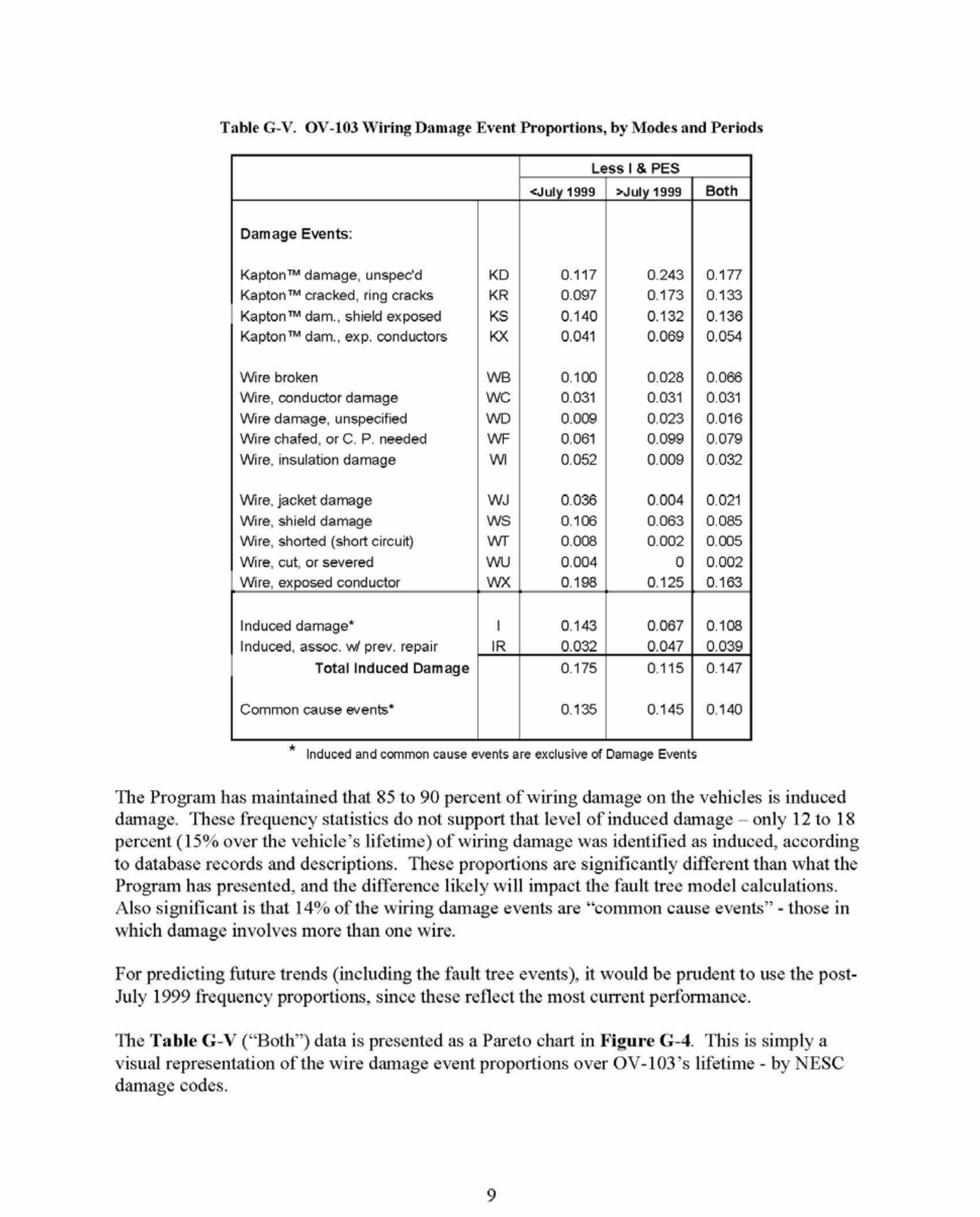


Table G-V. OV-103 Wiring Damage Event Proportions, by Modes and Periods

		Less I & PES		
		<July 1999	>July 1999	Both
Damage Events:				
Kapton™ damage, unspec'd	KD	0.117	0.243	0.177
Kapton™ cracked, ring cracks	KR	0.097	0.173	0.133
Kapton™ dam., shield exposed	KS	0.140	0.132	0.136
Kapton™ dam., exp. conductors	KX	0.041	0.069	0.054
Wire broken	WB	0.100	0.028	0.066
Wire, conductor damage	WC	0.031	0.031	0.031
Wire damage, unspecified	WD	0.009	0.023	0.016
Wire chafed, or C. P. needed	WF	0.061	0.099	0.079
Wire, insulation damage	WI	0.052	0.009	0.032
Wire, jacket damage	WJ	0.036	0.004	0.021
Wire, shield damage	WS	0.106	0.063	0.085
Wire, shorted (short circuit)	WT	0.008	0.002	0.005
Wire, cut, or severed	WU	0.004	0	0.002
Wire, exposed conductor	WX	0.198	0.125	0.163
Induced damage*	I	0.143	0.067	0.108
Induced, assoc. w/ prev. repair	IR	0.032	0.047	0.039
Total Induced Damage		0.175	0.115	0.147
Common cause events*		0.135	0.145	0.140

* Induced and common cause events are exclusive of Damage Events

The Program has maintained that 85 to 90 percent of wiring damage on the vehicles is induced damage. These frequency statistics do not support that level of induced damage – only 12 to 18 percent (15% over the vehicle's lifetime) of wiring damage was identified as induced, according to database records and descriptions. These proportions are significantly different than what the Program has presented, and the difference likely will impact the fault tree model calculations. Also significant is that 14% of the wiring damage events are "common cause events" - those in which damage involves more than one wire.

For predicting future trends (including the fault tree events), it would be prudent to use the post-July 1999 frequency proportions, since these reflect the most current performance.

The **Table G-V** ("Both") data is presented as a Pareto chart in **Figure G-4**. This is simply a visual representation of the wire damage event proportions over OV-103's lifetime - by NESC damage codes.

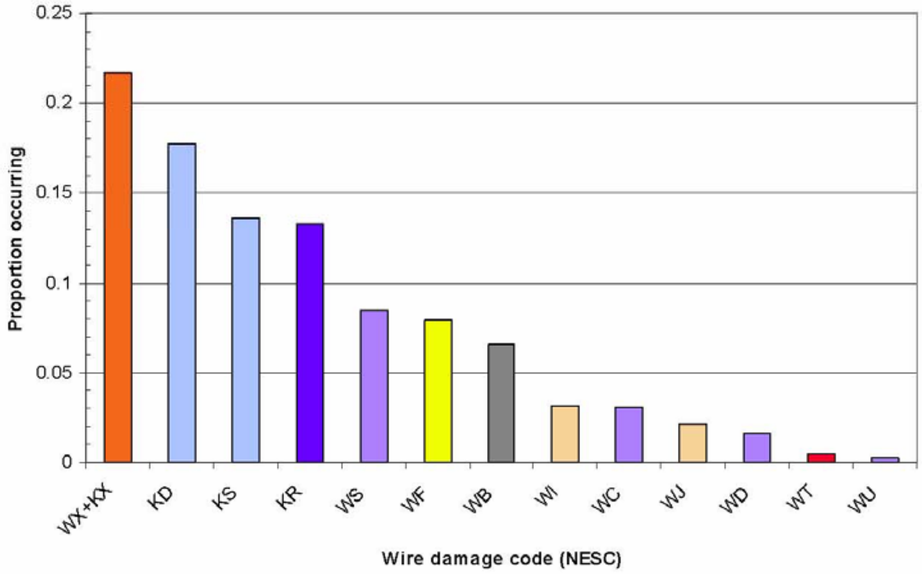
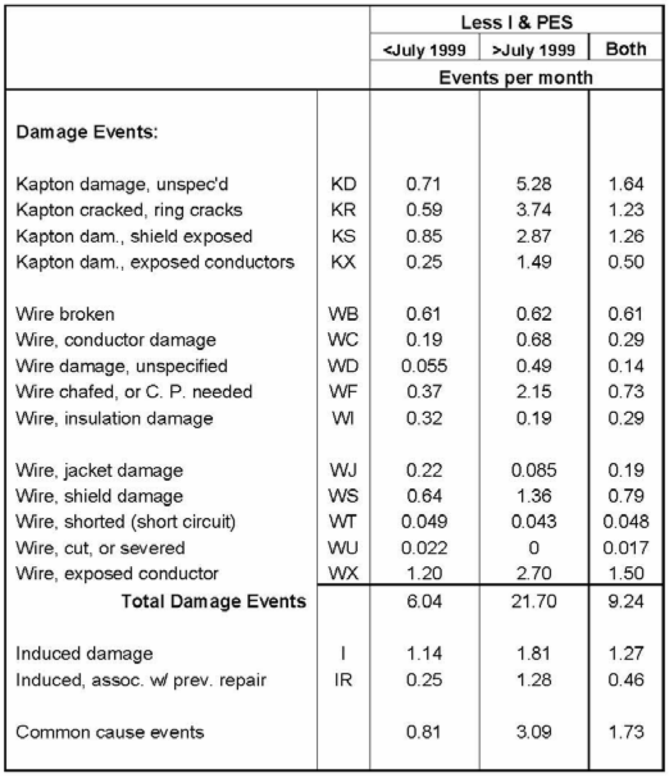


Figure G-4. Pareto chart for OV-103 wiring damage events over the vehicle's lifetime. (See Table G-III for code descriptions).

Tables G-IV and **G-V** statistics can be deceiving. What are apparent similarities in occurrence frequencies between pre- and post-July 1999, in fact, occur over different time periods. Post-July 1999 covers a time approximately one fourth the pre-July 1999 period – 47 months versus 183 months.

Table G-VI presents *"normalized"* occurrence frequencies, where for each period the numbers of occurrences are divided by the total number of months. This allows a less biased comparison between before- and after-July 1999 events. **Table G-VI** shows that for most all wire damage events (modes), the normalized occurrence *rate* (total occurrences divided by total months) increased by two to nine times after the July 1999 "wiring stand-down". Exceptions were *broken wires*, *Kapton™ damage – shield exposed*, *wire jacket* and *insulation damage*: broken wires and Kapton™ shield exposed remained the same, whereas jacket and insulation damage normalized rates decreased by about one half. All non-induced wiring damage events ("Total Damage Events") were detected at about three and one half times greater *frequency* (normalized) after the stand-down. This is *not consistent* with the Program-cited "six-fold increase" in detected wiring damage events, at least for OV-103.

Table G-VI. Normalized occurrence rates for OV-103 Wiring Damage Events, reported as event mean occurrences per month



		Less I & PES		
		<July 1999	>July 1999	Both
		Events per month		
Damage Events:				
Kapton damage, unspec'd	KD	0.71	5.28	1.64
Kapton cracked, ring cracks	KR	0.59	3.74	1.23
Kapton dam., shield exposed	KS	0.85	2.87	1.26
Kapton dam., exposed conductors	KX	0.25	1.49	0.50
Wire broken	WB	0.61	0.62	0.61
Wire, conductor damage	WC	0.19	0.68	0.29
Wire damage, unspecified	WD	0.055	0.49	0.14
Wire chafed, or C. P. needed	WF	0.37	2.15	0.73
Wire, insulation damage	WI	0.32	0.19	0.29
Wire, jacket damage	WJ	0.22	0.085	0.19
Wire, shield damage	WS	0.64	1.36	0.79
Wire, shorted (short circuit)	WT	0.049	0.043	0.048
Wire, cut, or severed	WU	0.022	0	0.017
Wire, exposed conductor	WX	1.20	2.70	1.50
Total Damage Events		6.04	21.70	9.24
Induced damage	I	1.14	1.81	1.27
Induced, assoc. w/ prev. repair	IR	0.25	1.28	0.46
Common cause events		0.81	3.09	1.73

IV. The STS Wire Inspection/Maintenance Process and OV-103 Wiring Damage Events

An initial analysis was performed on Program data [11]. These records compiled wire and interconnect short circuits over the Program's lifetime, for all vehicles, from the PRACA[†] database and were presented in May 2004. Since these data likely had multiple failure modes and "missing data", Crow-AMSAA[‡] (CA) is the appropriate analysis tool [12]. Data covered 1983 through 2004 and listed wire damage and short (circuit) events. The resulting CA plot[§] is shown in Figure G-5.

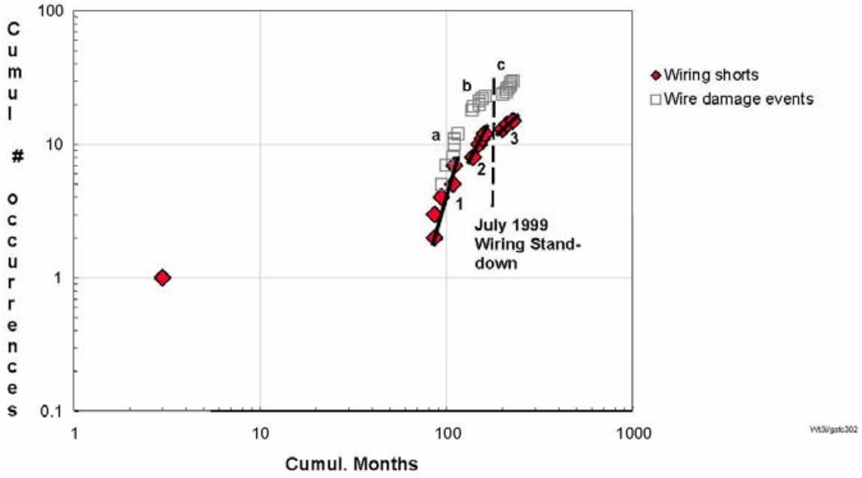


Figure G-5. Crow-AMSAA plot of STS Orbiter Interconnect Short Circuits

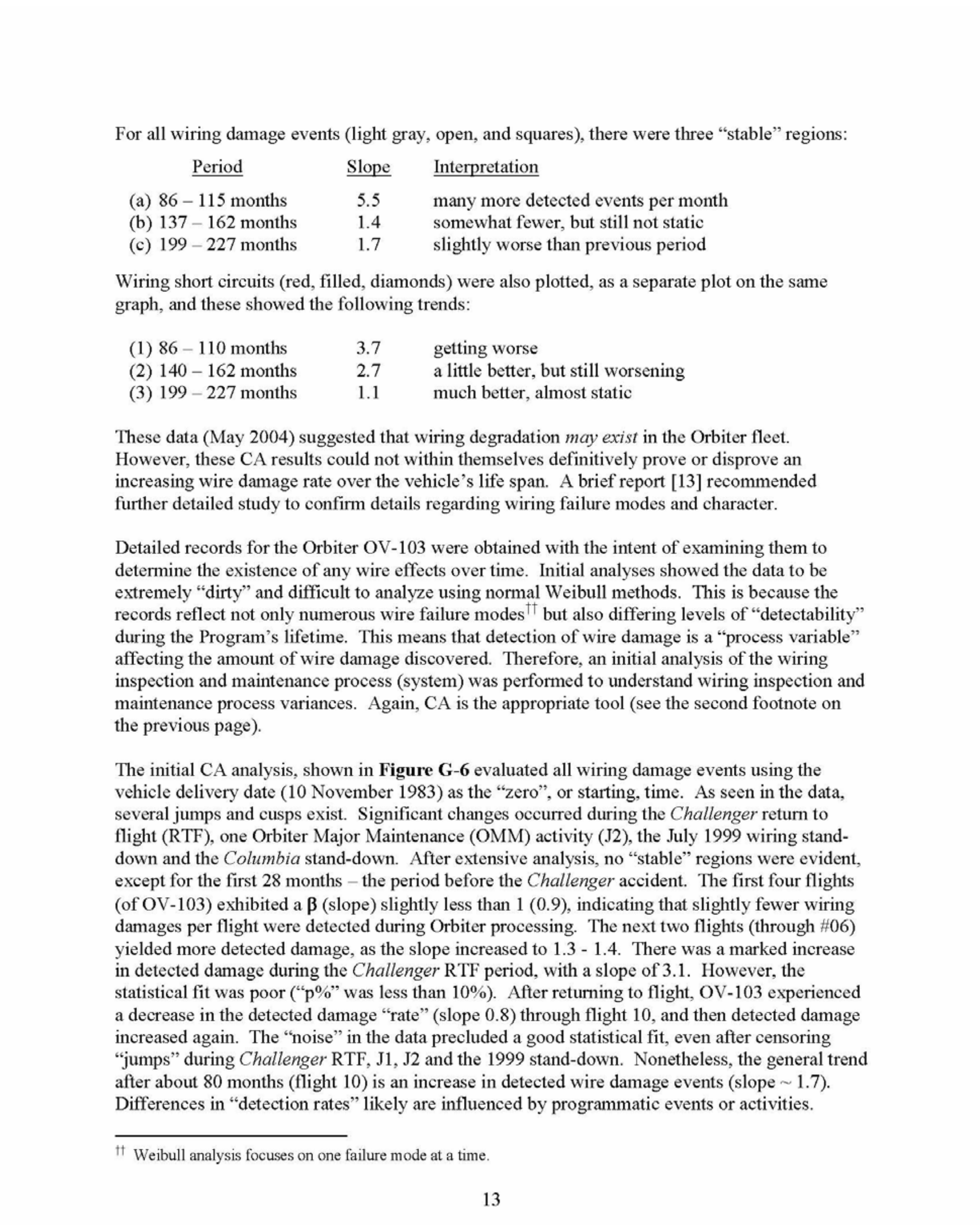
The one wiring short circuit to the extreme left on the plot was a significant flight occurrence in March 1983. Other data were "missing" until approximately 86 months later.[**] The 1983 datum was suspended for the CA statistical analyses.

[†] PRACA is the Problem Reporting And Corrective Action database.

[‡] Crow-AMSAA (CA) analysis is an analysis tool originally developed to track reliability growth. It has found applications in tracking and trending reliability, safety, maintainability, and warranty events in numerous industries. It is particularly useful because it can handle "dirty data" including missing data, and mixtures of failure modes. CA "looks at" the entire system, which for our purposes means the wiring damage event occurrences and the inspection/detection/maintenance/reporting process. Straight lines on the plot define "stable" regions wherein the process follows a well-defined occurrence distribution; slopes indicate improvement (slope <1) or deterioration (slope >1) or no change (slope ~ 1). Jumps or cusps indicate some change having occurred in the process.

[§] Analyses were performed using *SuperSmith Visual*™ software (Fulton Findings) and results ported to *Excel*™ (Microsoft).

[**] Data prior to ca. 1989 had not been entered into the electronic database; written records had been archived and were not researched.



For all wiring damage events (light gray, open, and squares), there were three "stable" regions:

Period	Slope	Interpretation
(a) 86 – 115 months	5.5	many more detected events per month
(b) 137 – 162 months	1.4	somewhat fewer, but still not static
(c) 199 – 227 months	1.7	slightly worse than previous period

Wiring short circuits (red, filled, diamonds) were also plotted, as a separate plot on the same graph, and these showed the following trends:

(1) 86 – 110 months	3.7	getting worse
(2) 140 – 162 months	2.7	a little better, but still worsening
(3) 199 – 227 months	1.1	much better, almost static

These data (May 2004) suggested that wiring degradation *may exist* in the Orbiter fleet. However, these CA results could not within themselves definitively prove or disprove an increasing wire damage rate over the vehicle's life span. A brief report [13] recommended further detailed study to confirm details regarding wiring failure modes and character.

Detailed records for the Orbiter OV-103 were obtained with the intent of examining them to determine the existence of any wire effects over time. Initial analyses showed the data to be extremely "dirty" and difficult to analyze using normal Weibull methods. This is because the records reflect not only numerous wire failure modes[††] but also differing levels of "detectability" during the Program's lifetime. This means that detection of wire damage is a "process variable" affecting the amount of wire damage discovered. Therefore, an initial analysis of the wiring inspection and maintenance process (system) was performed to understand wiring inspection and maintenance process variances. Again, CA is the appropriate tool (see the second footnote on the previous page).

The initial CA analysis, shown in **Figure G-6** evaluated all wiring damage events using the vehicle delivery date (10 November 1983) as the "zero", or starting, time. As seen in the data, several jumps and cusps exist. Significant changes occurred during the *Challenger* return to flight (RTF), one Orbiter Major Maintenance (OMM) activity (J2), the July 1999 wiring stand-down and the *Columbia* stand-down. After extensive analysis, no "stable" regions were evident, except for the first 28 months – the period before the *Challenger* accident. The first four flights (of OV-103) exhibited a **β** (slope) slightly less than 1 (0.9), indicating that slightly fewer wiring damages per flight were detected during Orbiter processing. The next two flights (through #06) yielded more detected damage, as the slope increased to 1.3 - 1.4. There was a marked increase in detected damage during the *Challenger* RTF period, with a slope of 3.1. However, the statistical fit was poor ("p%" was less than 10%). After returning to flight, OV-103 experienced a decrease in the detected damage "rate" (slope 0.8) through flight 10, and then detected damage increased again. The "noise" in the data precluded a good statistical fit, even after censoring "jumps" during *Challenger* RTF, J1, J2 and the 1999 stand-down. Nonetheless, the general trend after about 80 months (flight 10) is an increase in detected wire damage events (slope ~ 1.7). Differences in "detection rates" likely are influenced by programmatic events or activities.

[††] Weibull analysis focuses on one failure mode at a time.

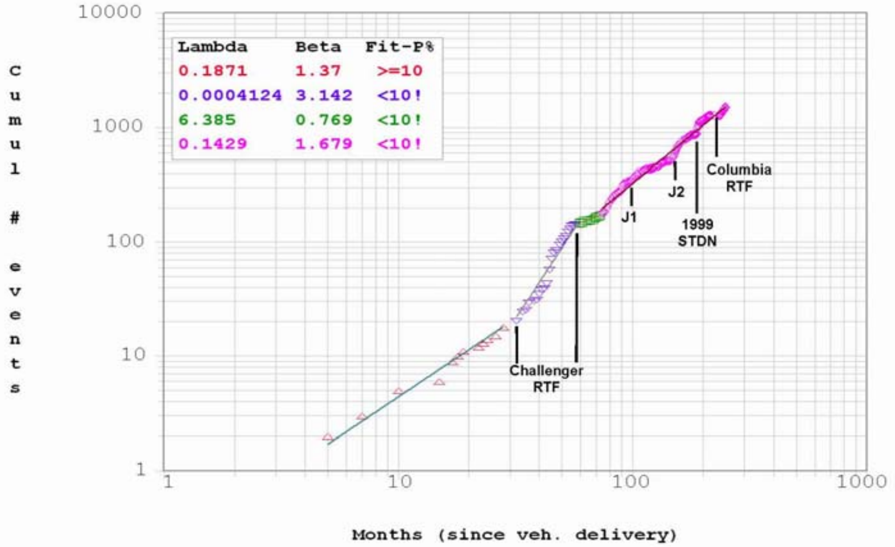


Figure G-6. Crow-AMSAA plot of all *detected* OV-103 wiring damage events, plotted by months since vehicle delivery

The **Figure G-6** data do not provide a good statistical basis for making any definitive conclusions (because of the poor statistical fit beyond 30 – 40 months).

Since the STS vehicles are "processed" between each flight, it seemed logical to plot wiring damage data by "vehicle flight number". This is the time between a given launch and just before the subsequent launch – it includes the flight time through landing (for any wire damage anomalies recorded during flight) and the following processing time (maintenance and inspections) leading up to the next flight. We have already seen that jumps in damage events occurred during or after significant vehicle events (**Figure G-6**), for example after the *Challenger* stand-down, two OMM activities ("J1" and "J2"), and the 1999 stand-down. To accommodate plotting cumulative data for these activities, the data was compiled using "relative flight number". The flight number after J1 is incremented by 1, after J2 by 2, and after the 1999 stand-down by 3 – so there appear to be 33 flights on the plot for OV-103's actual 30 flights. This CA plot by flight cycle is presented in **Figure G-7**, below. Numbers adjacent line segments are the slopes (**β**'s).

These data, in one sense, are taking a "coarser" look at the wiring inspection/maintenance process, since cumulative damage events are summed over entire flight cycles. Nonetheless, good statistical fits for various flight "segments" resulted throughout OV-103's lifetime. Likely, the effect is akin to moving average computations which tend to smooth out "noise" in data.

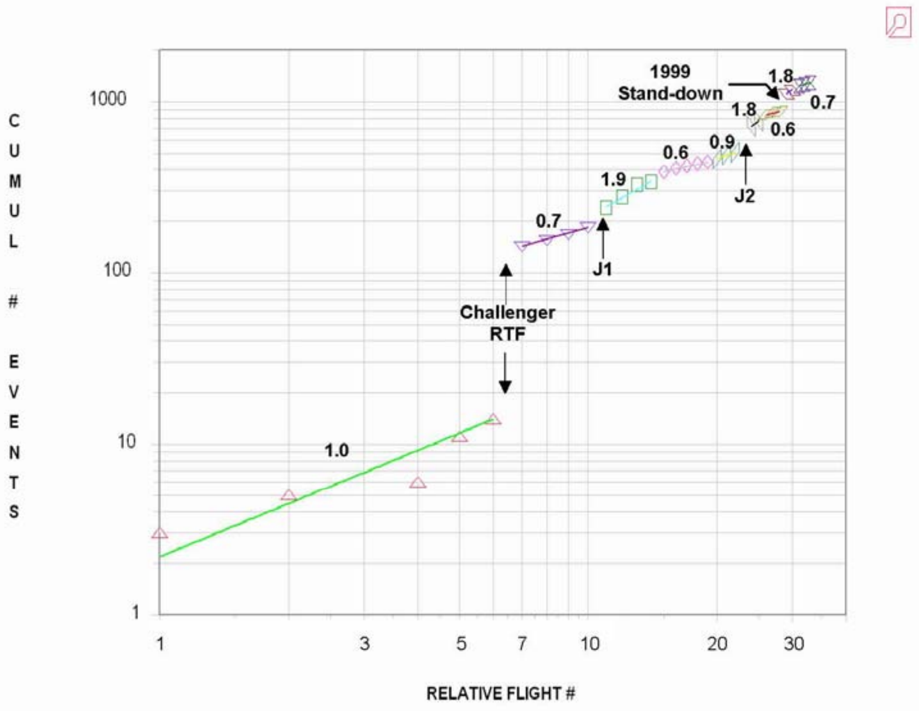


Figure G-7. Crow-AMSAA plot of OV-103 *detected* wiring damage events by vehicle flight number. Numbers above and below lines are slopes. "Relative flight numbers" are vehicle flight numbers incremented by 1 and 2 after J1 and J2, respectively.

In this plot, one can see the jumps at *Challenger* RTF, J1, J2, and the 1999 stand-down. Post-*Columbia*-accident data was not plotted. The initial (up to *Challenger*) detection rate was static (slope ~ 1), compared to the 1.4 seen in the "by month" data. After *Challenger* RTF, the per-flight data exhibited the same slope of decreased wire damage detection (0.7 vs. 0.8 for the "by month" data) until the J1 OMM activity. After J1, detected events increased for four flights and then decreased for the next five flights (0.6 slope). There was an increase in detected events for flights 19 through 21. An expected jump occurred for J2 OMM. Then detected events changed between increased detection (slope 1.8) and decreased detection (slope 0.6) until the 1999 stand-down. It subsequently followed the same pattern after the 1999 stand-down – increased detection (1.8) then reduced detection (0.7). The inspection/detection process appears to oscillate between enhanced and diminished detection since the J1 OMM activity.

The above plot is a "traditional" CA plot, in which it is easy to see improvement or deterioration and jumps or cusps within trends signifying process changes. In fact, if a process exhibits "stable" behavior (one fitting a straight line for "a long time"), future performance can be read directly from the plot. For example, if the OV-103 wiring damage detection process was *stable*, future performance could be predicted by a simple linear extrapolation to future flights. This, of course, assumes that no jumps or cusps occur within the future period.

Another way of looking at the same data is to plot the events as an *occurrence rate* (failure rate if the plotted events are failures) versus cumulative time (flight cycles, in our case). This is shown in **Figure G-8**.

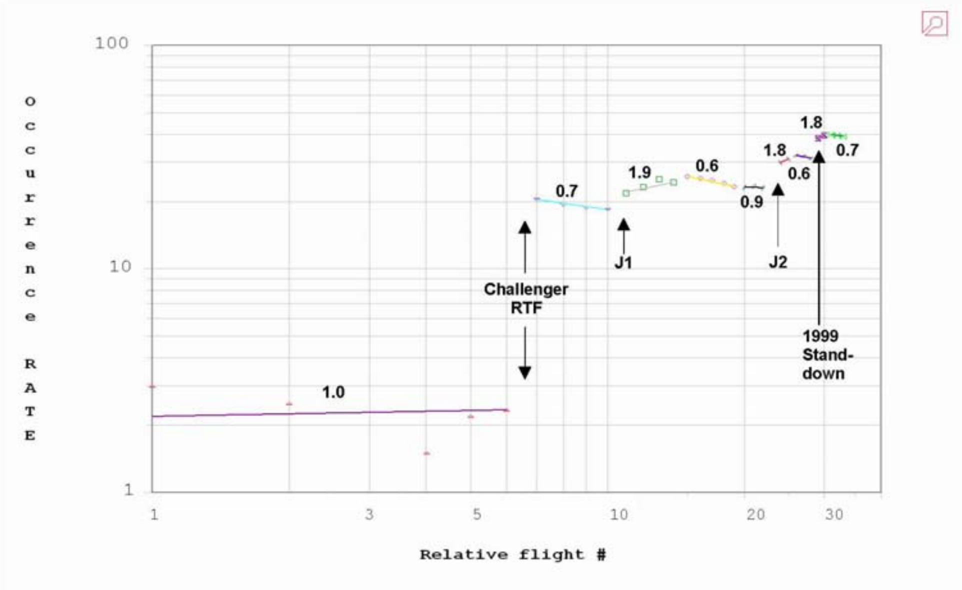
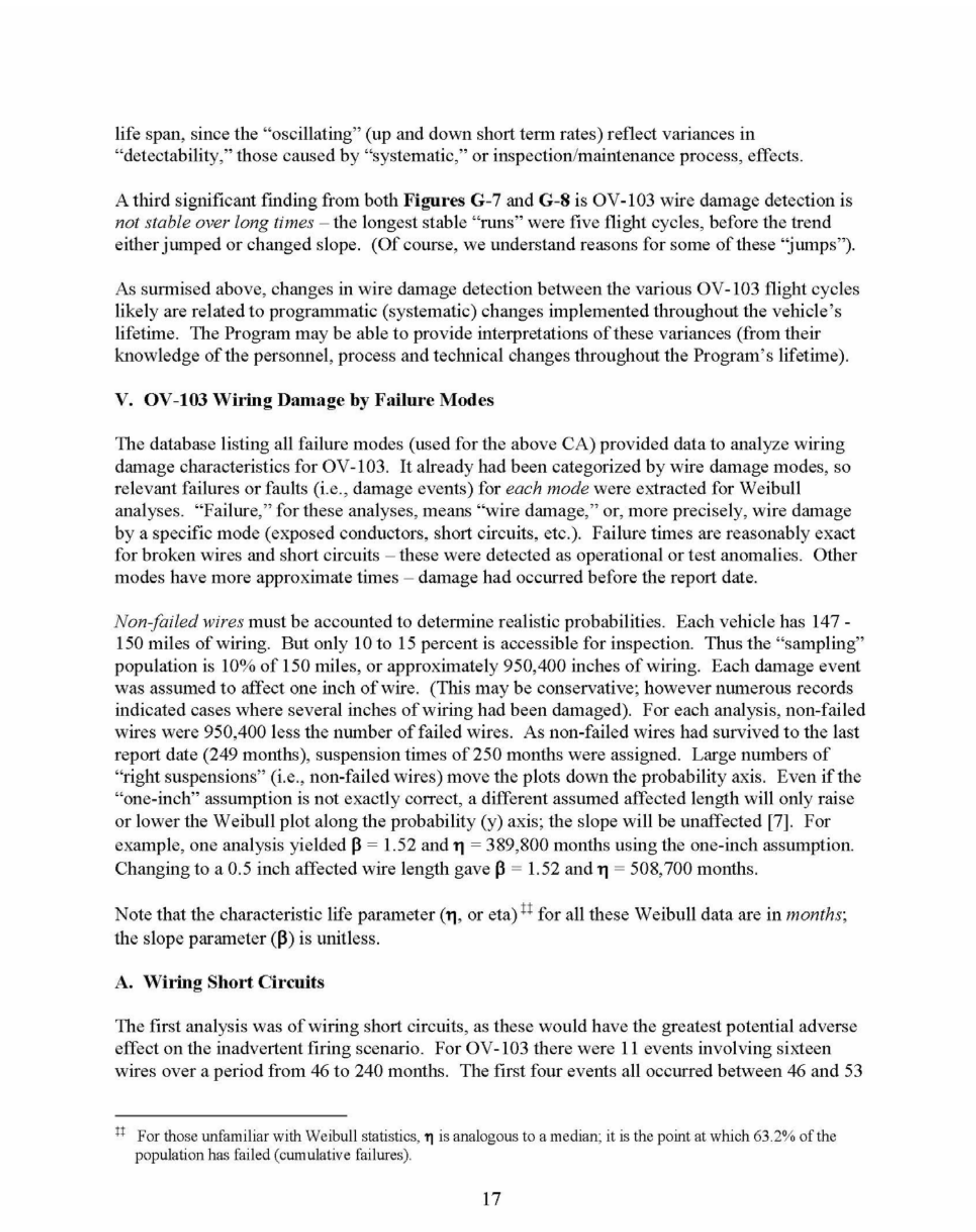


Figure G-8. OV-103 Wiring Damage Events (By Flight Cycle) Plotted as Occurrence Rates, from CA Plot

The **Figure G-8** data are the event occurrence *rates* (analogous to failure rates) plotted per (cumulative) flight cycle. For this presentation, a "flat" line means the process is static (not changing with time), an upward slope (to the right) means events are occurring more frequently with time (more events detected per flight cycle), and a downward slope means fewer events occurring with time (fewer detected per flight cycle). This plot reflects the same trends shown in the "traditional" CA plot (**Figure G-7**) and it is easier to distinguish between "improvement" and "deterioration".

A significant finding is that the claimed six-fold increase in wiring damage detection after the 1999 stand-down is not justified. Prior to the stand-down (the 1.8 and 0.6 slopes before relative flight 28 - actual flight 26) the wiring event detection rate was approximately 30 events per cycle. After the stand-down (1.8 and 0.7 slopes), it was about 40 events per cycle, an increase of only 1.3 times. Another significant finding is that the detected event occurrence rate gradually increased after the *Challenger* RTF: the detected event rate changed from about 20 per flight to 40 per flight. This gradual increase likely represents an increase in wiring damage related to its



life span, since the "oscillating" (up and down short term rates) reflect variances in "detectability," those caused by "systematic," or inspection/maintenance process, effects.

A third significant finding from both **Figures G-7** and **G-8** is OV-103 wire damage detection is *not stable over long times* – the longest stable "runs" were five flight cycles, before the trend either jumped or changed slope. (Of course, we understand reasons for some of these "jumps").

As surmised above, changes in wire damage detection between the various OV-103 flight cycles likely are related to programmatic (systematic) changes implemented throughout the vehicle's lifetime. The Program may be able to provide interpretations of these variances (from their knowledge of the personnel, process and technical changes throughout the Program's lifetime).

V. OV-103 Wiring Damage by Failure Modes

The database listing all failure modes (used for the above CA) provided data to analyze wiring damage characteristics for OV-103. It already had been categorized by wire damage modes, so relevant failures or faults (i.e., damage events) for *each mode* were extracted for Weibull analyses. "Failure," for these analyses, means "wire damage," or, more precisely, wire damage by a specific mode (exposed conductors, short circuits, etc.). Failure times are reasonably exact for broken wires and short circuits – these were detected as operational or test anomalies. Other modes have more approximate times – damage had occurred before the report date.

Non-failed wires must be accounted to determine realistic probabilities. Each vehicle has 147 - 150 miles of wiring. But only 10 to 15 percent is accessible for inspection. Thus the "sampling" population is 10% of 150 miles, or approximately 950,400 inches of wiring. Each damage event was assumed to affect one inch of wire. (This may be conservative; however numerous records indicated cases where several inches of wiring had been damaged). For each analysis, non-failed wires were 950,400 less the number of failed wires. As non-failed wires had survived to the last report date (249 months), suspension times of 250 months were assigned. Large numbers of "right suspensions" (i.e., non-failed wires) move the plots down the probability axis. Even if the "one-inch" assumption is not exactly correct, a different assumed affected length will only raise or lower the Weibull plot along the probability (y) axis; the slope will be unaffected [7]. For example, one analysis yielded $\boldsymbol{\beta}$ = 1.52 and $\boldsymbol{\eta}$ = 389,800 months using the one-inch assumption. Changing to a 0.5 inch affected wire length gave $\boldsymbol{\beta}$ = 1.52 and $\boldsymbol{\eta}$ = 508,700 months.

Note that the characteristic life parameter ($\boldsymbol{\eta}$, or eta)[‡‡] for all these Weibull data are in *months*; the slope parameter ($\boldsymbol{\beta}$) is unitless.

A. Wiring Short Circuits

The first analysis was of wiring short circuits, as these would have the greatest potential adverse effect on the inadvertent firing scenario. For OV-103 there were 11 events involving sixteen wires over a period from 46 to 240 months. The first four events all occurred between 46 and 53

[‡‡] For those unfamiliar with Weibull statistics, $\boldsymbol{\eta}$ is analogous to a median; it is the point at which 63.2% of the population has failed (cumulative failures).

months during the *Challenger* RTF. An initial Weibull plot showed an apparent bimodal distribution, with these first five wire failures (four events) occurring as one set having a high **β** (6.0). Interval analysis was tried, but yielded a poor fit. Four events occurring "almost simultaneously" (compared to the entire 300 months of the time axis) is analogous to "inspection data" [14], where failure points appear "stacked". Using the "interval option" produced a poor fit (3 to 6 % pve). However, interval data was simulated by suspending the first three failures and using the "standard" analysis. This produced the Weibull plot shown as **Figure G-9**.

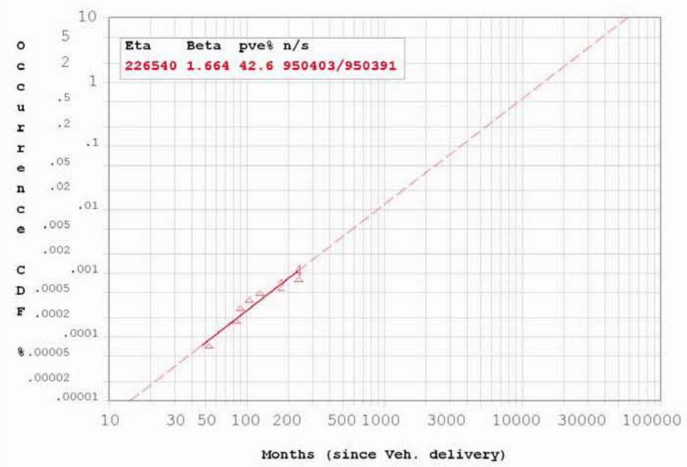


Figure G- 9. Weibull plot of OV-103 wiring short-circuit events. The Weibull slope indicates early wear-out failures are occurring.

The Weibull parameters (**β** = 1.7 and **η** = 226,500 months) indicate an early wear-out failure mode, that is, the failure rate is increasing with time, albeit at a slower rate than "true" wear-out (**β** greater than 4). Thus for wire short circuits, there *is* an effect in that the failure (or occurrence) rate is increasing with time. The above Weibull parameters can be inserted into the fault tree model to replace the existing CFR assumption; this will more accurately reflect wire short circuit occurrences, at least for OV-103.

B. Wiring Exposed Conductors

Data for both "wire with exposed conductors" and "Kapton™ damage with exposed conductors" (WX and KX codes) were combined to derive this failure distribution. Both modes create "exposed conductors", a primary (bottom-level) event for the inadvertent firing scenario. The initial plot, using all 342 exposed conductor events, was very "dirty" and not solvable, even after numerous attempts at suspending various portions. The plot was not unlike that of **Figure G-6**'s data. Abernethy suggests the Kaplan-Meier (K-M) survival function as appropriate for "…large data sets of either or both failures and suspensions" [15]. The K-M survival function has been used in the medical industry for years. It is *non-parametric*, not requiring a fit to any distribution. Since it computes "survivals", its complement is a "failure" function which can be analyzed using the Weibull distribution. The exposed conductor data were recompiled to a K-M format, using accumulated "survivors" (total number of wires less the "failed" and censored ones) at each flight cycle.

The resulting K-M Weibull fit was excellent, yielding **Figure G-10**. Exposed conductors initially fail as a near-CFR distribution (β = 0.9) until about 78 months (six and a half years) when early wear-out failures (β = 2.2) "take over". [Exact parameters from the plot can be used in the fault tree calculations or other predictions].

Exposed conductors are a primary concern regarding the wiring contributions to inadvertent RJD firing. If the Program replaces RJD control wiring (as proposed in the NESC briefings), only randomly occurring exposed conductor failures would be expected for approximately six and a half years of vehicle life after the wiring is replaced. (This assumes that the replaced wiring is equivalent to the existing wiring in the vehicle).

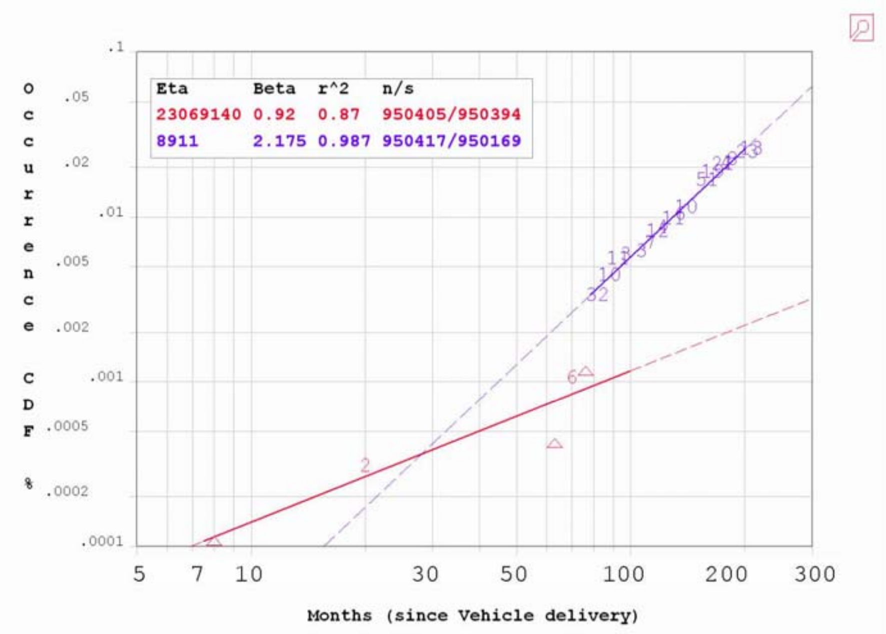


Figure G-10. Weibull plot of Kaplan-Meier data for OV-103 exposed conductor events. Earlier distribution is a near-random failure rate; later distribution is early wear-out.

C. Kapton™ Cracks and Ring Cracks

Data for Kapton™ cracks and "ring" cracks (KR code) were analyzed using the K-M function (see **B**, above). The first analysis, using all data as one set gave a poor fit ($r^2 = 0.74$). However, the data pattern was similar to exposed conductors, above. There was an initial "flat" distribution (**β** = 0.4 **η** = 2 x 10^{15} months) out to about 91 months followed by an early wear-out distribution (**β** = 1.9 **η** = 23,320 months). The Weibull plot is shown as **Figure G-11**.

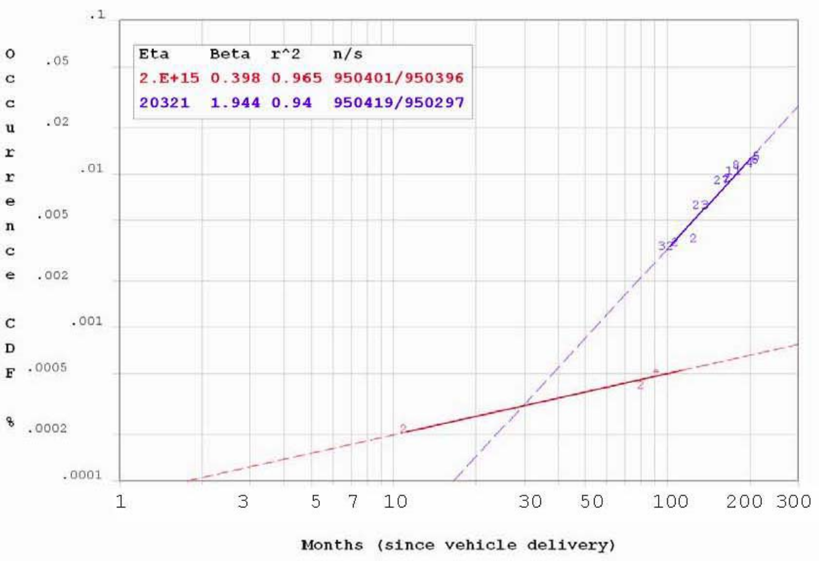


Figure G-11. Weibull plot (K-M) for OV-103 Kapton™ cracking and ring cracks. Early failures are infant mortals; later are early wear-outs.

D. Other Kapton™ Damage – Exposed Shield and Not-Specified

NESC coding had categories for "Kapton™ damage that exposed wire shielding" (KS) and "Kapton™ damage unspecified" (KD) - damage for which the description did not specify in enough detail to assign the event to one of the other categories. As these were the two remaining Kapton™ damage categories, they were combined and analyzed using a Weibull/K-M plot. For these modes, the data gave a good fit (0.95 r^2), although failure points deviated from the fit line above 90 months. Dividing the data at less than 89 months and greater than 93 months improved the "upper" fit to 0.99 and the weighted composite fit to 0.98. Either fit is equivalent, since the **β**'s and **η**'s were similar for all:

		β	η	r^2	
Fit using all data:		2.88	2630	0.95	
Fit separating data:	(a)	2.89	2770	0.99	
	(b)	2.92	2700	0.94	(0.98 – weighted composite)

The plot using the "separated" data is shown as **Figure G-12**. In this case, there was no initial "flat" distribution – early wear-out events commenced at about 60 months.

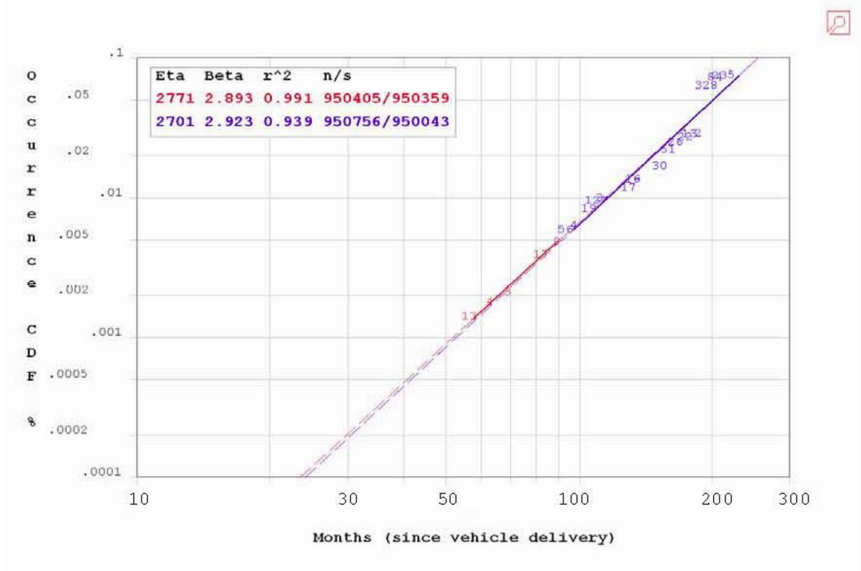


Figure G-12. Weibull Plot of Other Kapton™ Damage Events (KD and KS)

E. Wire Chaffing Events

Wire chafing events include instances where inspectors discovered either wires which had been chafed or wires that required chafe protection (that is, there were indications that chafing protection would be needed to prevent further damage). These were analyzed using a Weibull plot of the K-M survival function for wire chafe events and the results were similar to other damage modes: a "flat" Weibull (infant mortals) followed by early wear-outs after about 80 months. These results are shown in **Figure G-13**.

F. Broken Wires

A broken wire was involved in at least one significant flight event (STS-93, see p. 7). Of 134 broken wire events, nearly half (64) were associated with ground lug or ground wire failures. All broken wires were analyzed using the K-M function and exhibited the initial "flat" Weibull seen in most other failure modes. However, during *Challenger* RTF and for subsequent flights until the first OMM (J1), broken wire failure incidence increased significantly. These returned to the early wear-outs (**β** ~ 2.3) seen for the other modes after J1. The plot is **Figure G-14**.

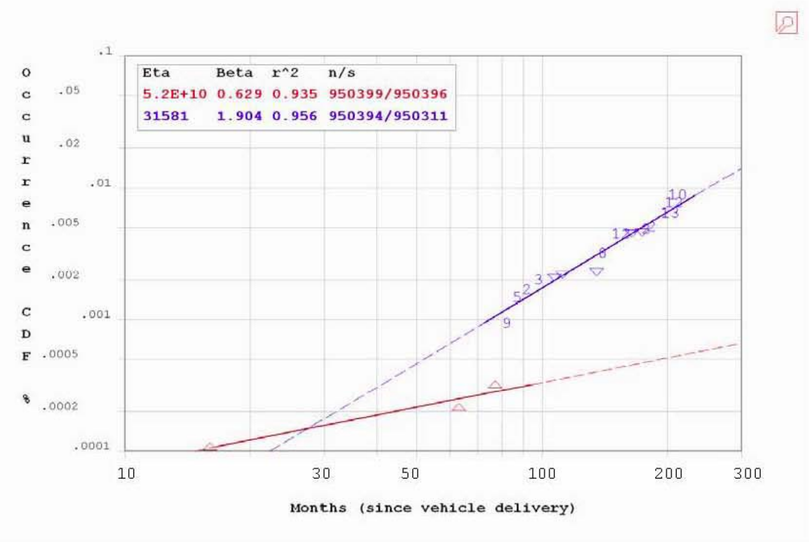


Figure G-13. Weibull (K-M) Plot of Wire Chaffing Events

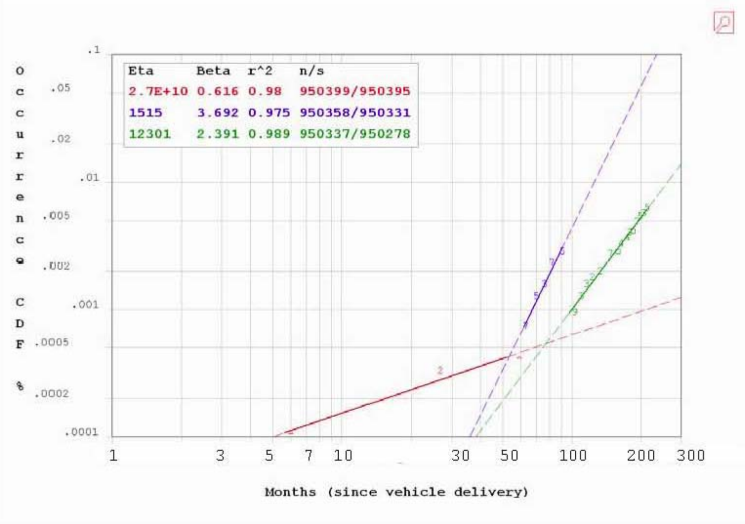
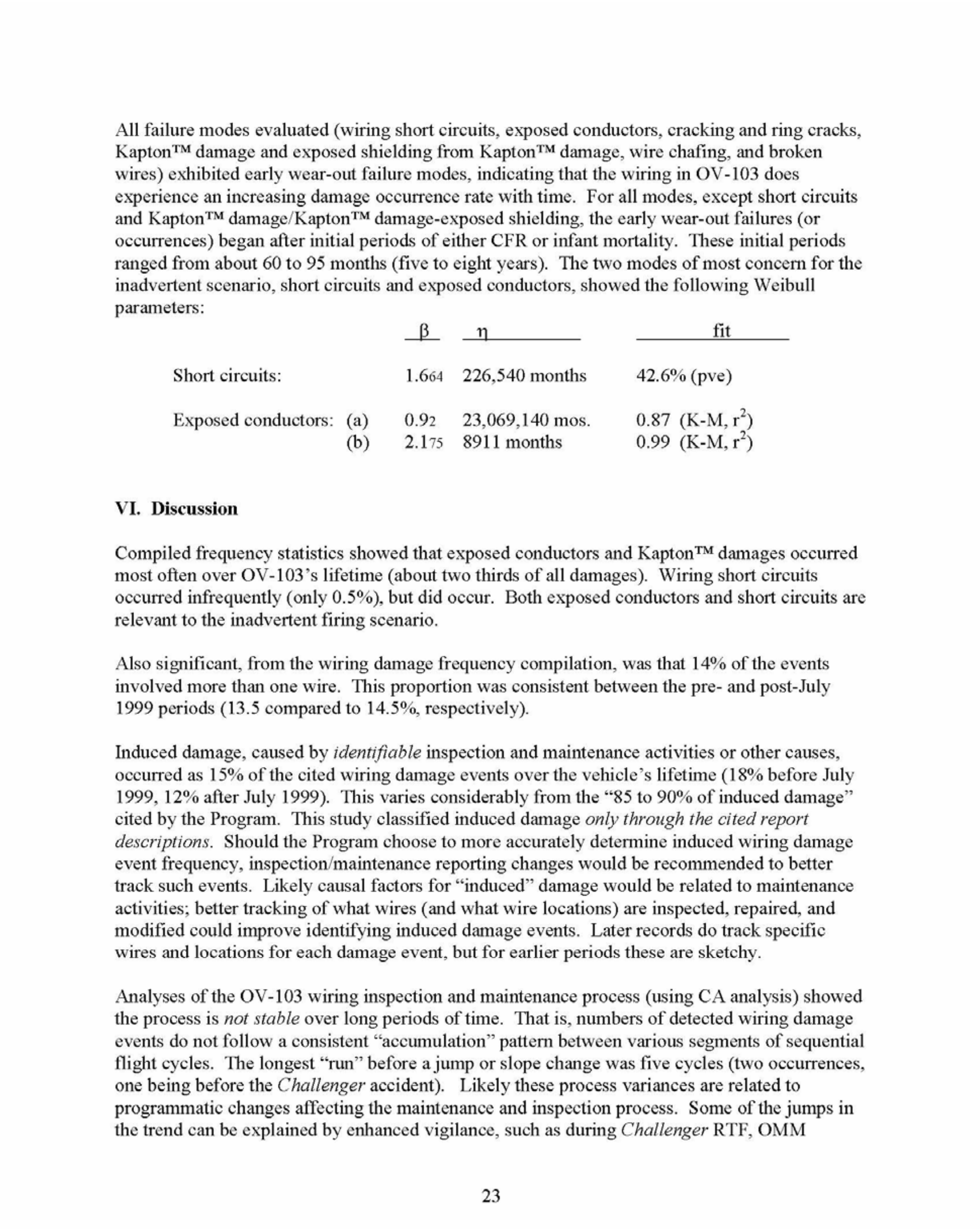


Figure G-14. Weibull (K-M) Plot of Broken Wire Events



All failure modes evaluated (wiring short circuits, exposed conductors, cracking and ring cracks, Kapton™ damage and exposed shielding from Kapton™ damage, wire chafing, and broken wires) exhibited early wear-out failure modes, indicating that the wiring in OV-103 does experience an increasing damage occurrence rate with time. For all modes, except short circuits and Kapton™ damage/Kapton™ damage-exposed shielding, the early wear-out failures (or occurrences) began after initial periods of either CFR or infant mortality. These initial periods ranged from about 60 to 95 months (five to eight years). The two modes of most concern for the inadvertent scenario, short circuits and exposed conductors, showed the following Weibull parameters:

		β	η	fit
Short circuits:		1.664	226,540 months	42.6% (pve)
Exposed conductors:	(a)	0.92	23,069,140 mos.	0.87 (K-M, r^2)
	(b)	2.175	8911 months	0.99 (K-M, r^2)

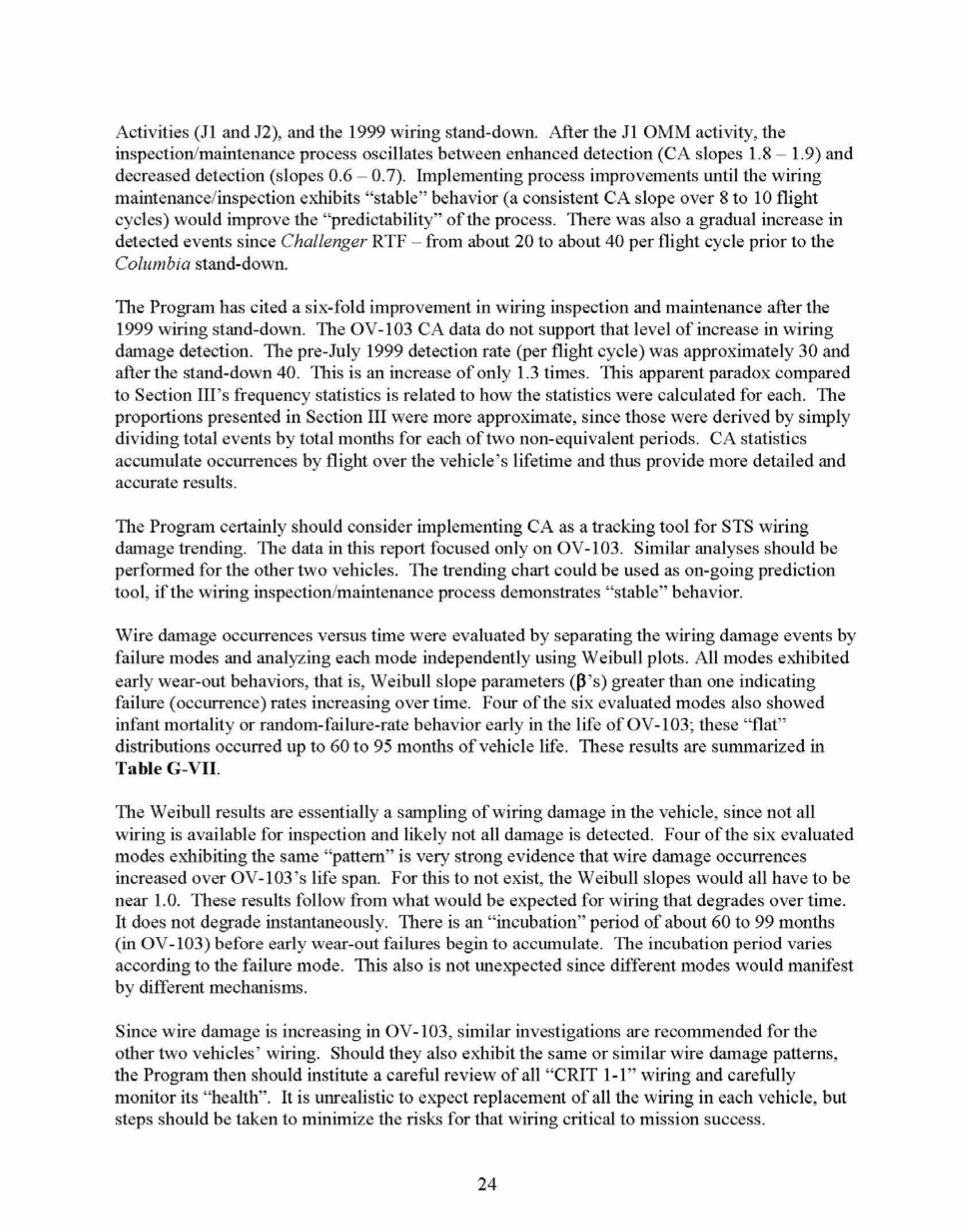
VI. Discussion

Compiled frequency statistics showed that exposed conductors and Kapton™ damages occurred most often over OV-103's lifetime (about two thirds of all damages). Wiring short circuits occurred infrequently (only 0.5%), but did occur. Both exposed conductors and short circuits are relevant to the inadvertent firing scenario.

Also significant, from the wiring damage frequency compilation, was that 14% of the events involved more than one wire. This proportion was consistent between the pre- and post-July 1999 periods (13.5 compared to 14.5%, respectively).

Induced damage, caused by *identifiable* inspection and maintenance activities or other causes, occurred as 15% of the cited wiring damage events over the vehicle's lifetime (18% before July 1999, 12% after July 1999). This varies considerably from the "85 to 90% of induced damage" cited by the Program. This study classified induced damage *only through the cited report descriptions*. Should the Program choose to more accurately determine induced wiring damage event frequency, inspection/maintenance reporting changes would be recommended to better track such events. Likely causal factors for "induced" damage would be related to maintenance activities; better tracking of what wires (and what wire locations) are inspected, repaired, and modified could improve identifying induced damage events. Later records do track specific wires and locations for each damage event, but for earlier periods these are sketchy.

Analyses of the OV-103 wiring inspection and maintenance process (using CA analysis) showed the process is *not stable* over long periods of time. That is, numbers of detected wiring damage events do not follow a consistent "accumulation" pattern between various segments of sequential flight cycles. The longest "run" before a jump or slope change was five cycles (two occurrences, one being before the *Challenger* accident). Likely these process variances are related to programmatic changes affecting the maintenance and inspection process. Some of the jumps in the trend can be explained by enhanced vigilance, such as during *Challenger* RTF, OMM



Activities (J1 and J2), and the 1999 wiring stand-down. After the J1 OMM activity, the inspection/maintenance process oscillates between enhanced detection (CA slopes 1.8 – 1.9) and decreased detection (slopes 0.6 – 0.7). Implementing process improvements until the wiring maintenance/inspection exhibits "stable" behavior (a consistent CA slope over 8 to 10 flight cycles) would improve the "predictability" of the process. There was also a gradual increase in detected events since *Challenger* RTF – from about 20 to about 40 per flight cycle prior to the *Columbia* stand-down.

The Program has cited a six-fold improvement in wiring inspection and maintenance after the 1999 wiring stand-down. The OV-103 CA data do not support that level of increase in wiring damage detection. The pre-July 1999 detection rate (per flight cycle) was approximately 30 and after the stand-down 40. This is an increase of only 1.3 times. This apparent paradox compared to Section III's frequency statistics is related to how the statistics were calculated for each. The proportions presented in Section III were more approximate, since those were derived by simply dividing total events by total months for each of two non-equivalent periods. CA statistics accumulate occurrences by flight over the vehicle's lifetime and thus provide more detailed and accurate results.

The Program certainly should consider implementing CA as a tracking tool for STS wiring damage trending. The data in this report focused only on OV-103. Similar analyses should be performed for the other two vehicles. The trending chart could be used as on-going prediction tool, if the wiring inspection/maintenance process demonstrates "stable" behavior.

Wire damage occurrences versus time were evaluated by separating the wiring damage events by failure modes and analyzing each mode independently using Weibull plots. All modes exhibited early wear-out behaviors, that is, Weibull slope parameters (β's) greater than one indicating failure (occurrence) rates increasing over time. Four of the six evaluated modes also showed infant mortality or random-failure-rate behavior early in the life of OV-103; these "flat" distributions occurred up to 60 to 95 months of vehicle life. These results are summarized in **Table G-VII**.

The Weibull results are essentially a sampling of wiring damage in the vehicle, since not all wiring is available for inspection and likely not all damage is detected. Four of the six evaluated modes exhibiting the same "pattern" is very strong evidence that wire damage occurrences increased over OV-103's life span. For this to not exist, the Weibull slopes would all have to be near 1.0. These results follow from what would be expected for wiring that degrades over time. It does not degrade instantaneously. There is an "incubation" period of about 60 to 99 months (in OV-103) before early wear-out failures begin to accumulate. The incubation period varies according to the failure mode. This also is not unexpected since different modes would manifest by different mechanisms.

Since wire damage is increasing in OV-103, similar investigations are recommended for the other two vehicles' wiring. Should they also exhibit the same or similar wire damage patterns, the Program then should institute a careful review of all "CRIT 1-1" wiring and carefully monitor its "health". It is unrealistic to expect replacement of all the wiring in each vehicle, but steps should be taken to minimize the risks for that wiring critical to mission success.

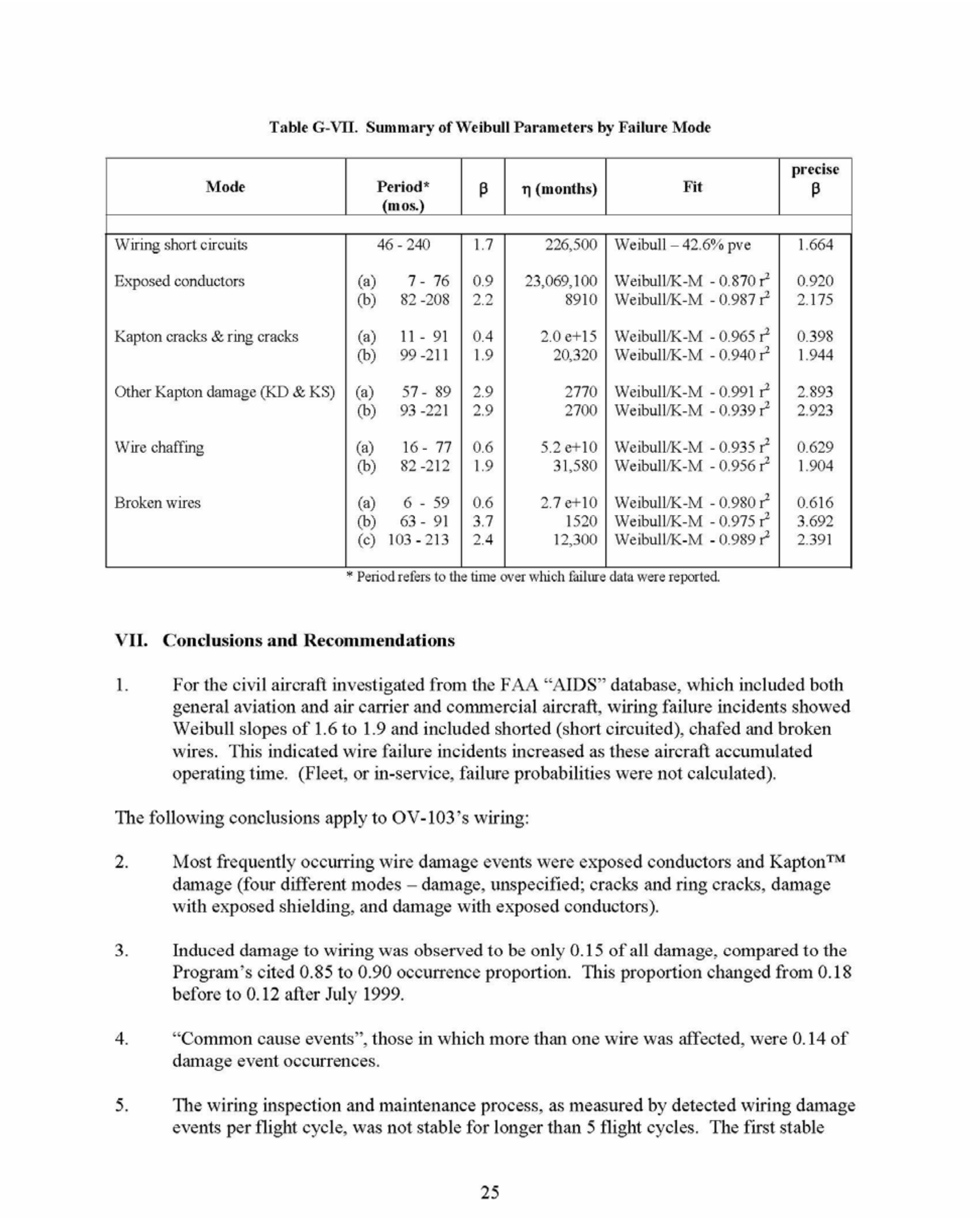


Table G-VII. Summary of Weibull Parameters by Failure Mode

Mode	Period* (mos.)	β	η (months)	Fit	precise β
Wiring short circuits	46 - 240	1.7	226,500	Weibull – 42.6% pve	1.664
Exposed conductors	(a) 7 - 76	0.9	23,069,100	Weibull/K-M - 0.870 r^2	0.920
	(b) 82 -208	2.2	8910	Weibull/K-M - 0.987 r^2	2.175
Kapton cracks & ring cracks	(a) 11 - 91	0.4	2.0 e+15	Weibull/K-M - 0.965 r^2	0.398
	(b) 99 -211	1.9	20,320	Weibull/K-M - 0.940 r^2	1.944
Other Kapton damage (KD & KS)	(a) 57 - 89	2.9	2770	Weibull/K-M - 0.991 r^2	2.893
	(b) 93 -221	2.9	2700	Weibull/K-M - 0.939 r^2	2.923
Wire chaffing	(a) 16 - 77	0.6	5.2 e+10	Weibull/K-M - 0.935 r^2	0.629
	(b) 82 -212	1.9	31,580	Weibull/K-M - 0.956 r^2	1.904
Broken wires	(a) 6 - 59	0.6	2.7 e+10	Weibull/K-M - 0.980 r^2	0.616
	(b) 63 - 91	3.7	1520	Weibull/K-M - 0.975 r^2	3.692
	(c) 103 - 213	2.4	12,300	Weibull/K-M - 0.989 r^2	2.391

* Period refers to the time over which failure data were reported.

VII. Conclusions and Recommendations

1. For the civil aircraft investigated from the FAA "AIDS" database, which included both general aviation and air carrier and commercial aircraft, wiring failure incidents showed Weibull slopes of 1.6 to 1.9 and included shorted (short circuited), chafed and broken wires. This indicated wire failure incidents increased as these aircraft accumulated operating time. (Fleet, or in-service, failure probabilities were not calculated).

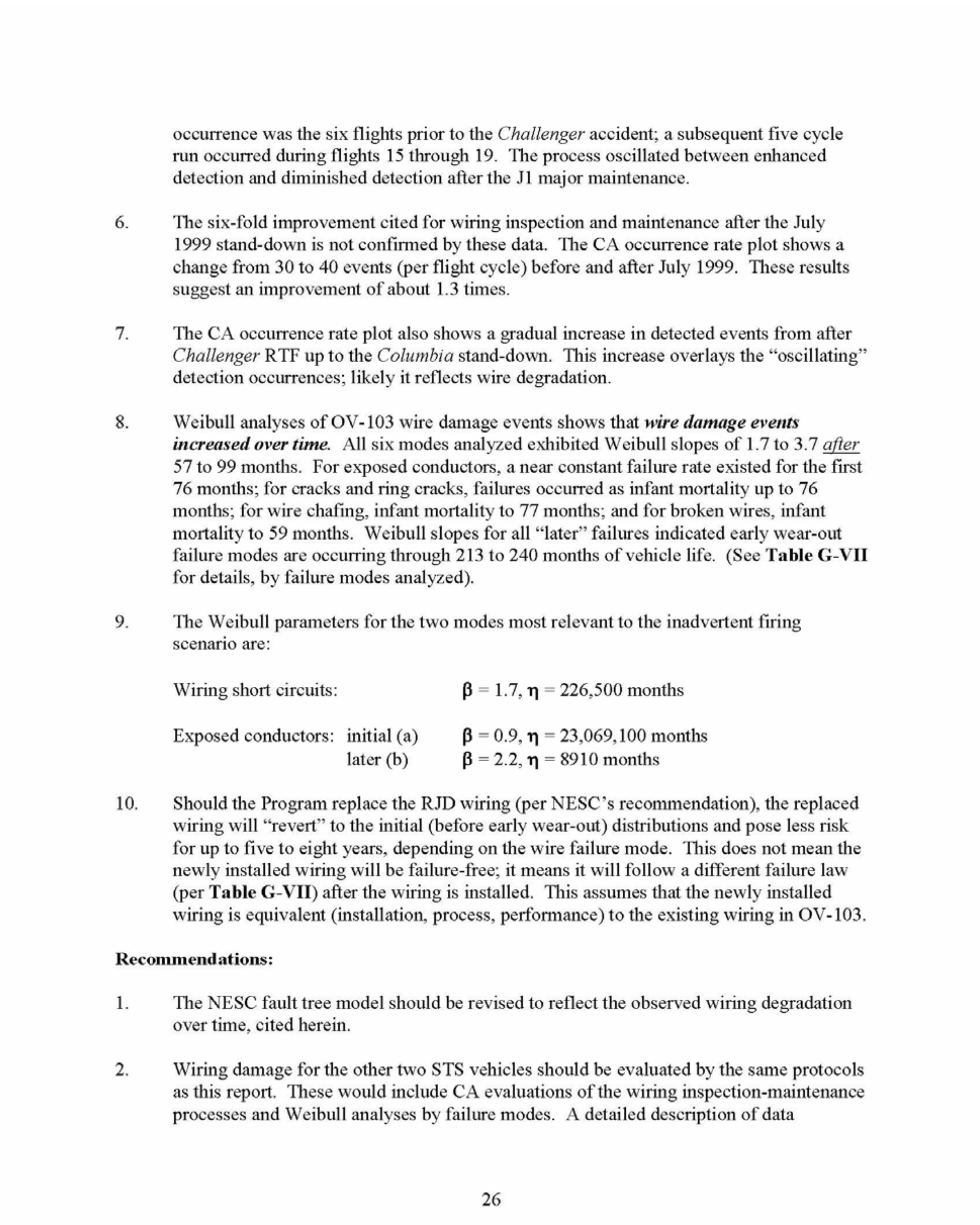
The following conclusions apply to OV-103's wiring:

2. Most frequently occurring wire damage events were exposed conductors and Kapton™ damage (four different modes – damage, unspecified; cracks and ring cracks, damage with exposed shielding, and damage with exposed conductors).

3. Induced damage to wiring was observed to be only 0.15 of all damage, compared to the Program's cited 0.85 to 0.90 occurrence proportion. This proportion changed from 0.18 before to 0.12 after July 1999.

4. "Common cause events", those in which more than one wire was affected, were 0.14 of damage event occurrences.

5. The wiring inspection and maintenance process, as measured by detected wiring damage events per flight cycle, was not stable for longer than 5 flight cycles. The first stable



occurrence was the six flights prior to the *Challenger* accident; a subsequent five cycle run occurred during flights 15 through 19. The process oscillated between enhanced detection and diminished detection after the J1 major maintenance.

6. The six-fold improvement cited for wiring inspection and maintenance after the July 1999 stand-down is not confirmed by these data. The CA occurrence rate plot shows a change from 30 to 40 events (per flight cycle) before and after July 1999. These results suggest an improvement of about 1.3 times.

7. The CA occurrence rate plot also shows a gradual increase in detected events from after *Challenger* RTF up to the *Columbia* stand-down. This increase overlays the "oscillating" detection occurrences; likely it reflects wire degradation.

8. Weibull analyses of OV-103 wire damage events shows that ***wire damage events increased over time.*** All six modes analyzed exhibited Weibull slopes of 1.7 to 3.7 *after* 57 to 99 months. For exposed conductors, a near constant failure rate existed for the first 76 months; for cracks and ring cracks, failures occurred as infant mortality up to 76 months; for wire chafing, infant mortality to 77 months; and for broken wires, infant mortality to 59 months. Weibull slopes for all "later" failures indicated early wear-out failure modes are occurring through 213 to 240 months of vehicle life. (See **Table G-VII** for details, by failure modes analyzed).

9. The Weibull parameters for the two modes most relevant to the inadvertent firing scenario are:

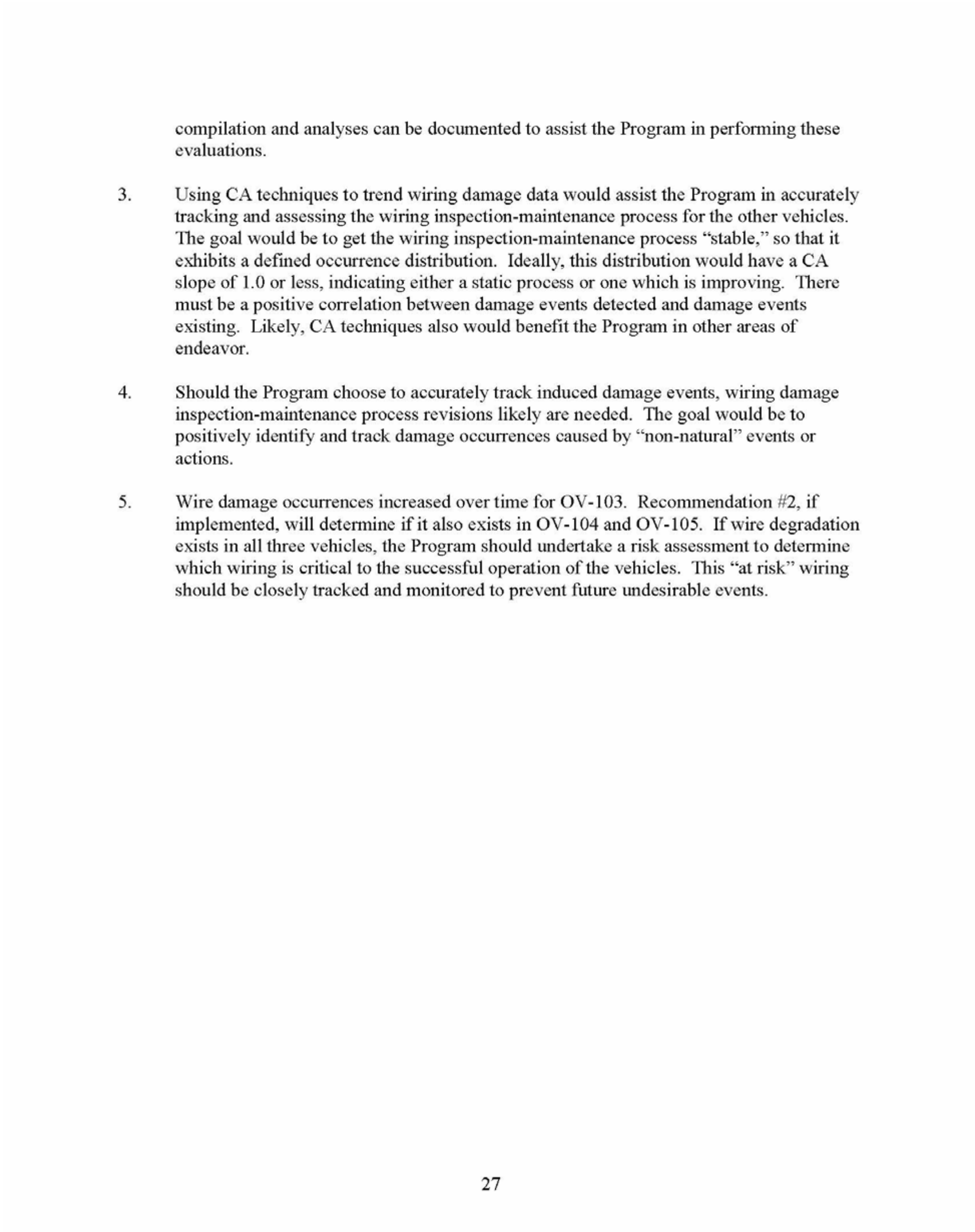
Wiring short circuits:		$\beta = 1.7$, $\eta = 226{,}500$ months
Exposed conductors:	initial (a)	$\beta = 0.9$, $\eta = 23{,}069{,}100$ months
	later (b)	$\beta = 2.2$, $\eta = 8910$ months

10. Should the Program replace the RJD wiring (per NESC's recommendation), the replaced wiring will "revert" to the initial (before early wear-out) distributions and pose less risk for up to five to eight years, depending on the wire failure mode. This does not mean the newly installed wiring will be failure-free; it means it will follow a different failure law (per **Table G-VII**) after the wiring is installed. This assumes that the newly installed wiring is equivalent (installation, process, performance) to the existing wiring in OV-103.

Recommendations:

1. The NESC fault tree model should be revised to reflect the observed wiring degradation over time, cited herein.

2. Wiring damage for the other two STS vehicles should be evaluated by the same protocols as this report. These would include CA evaluations of the wiring inspection-maintenance processes and Weibull analyses by failure modes. A detailed description of data

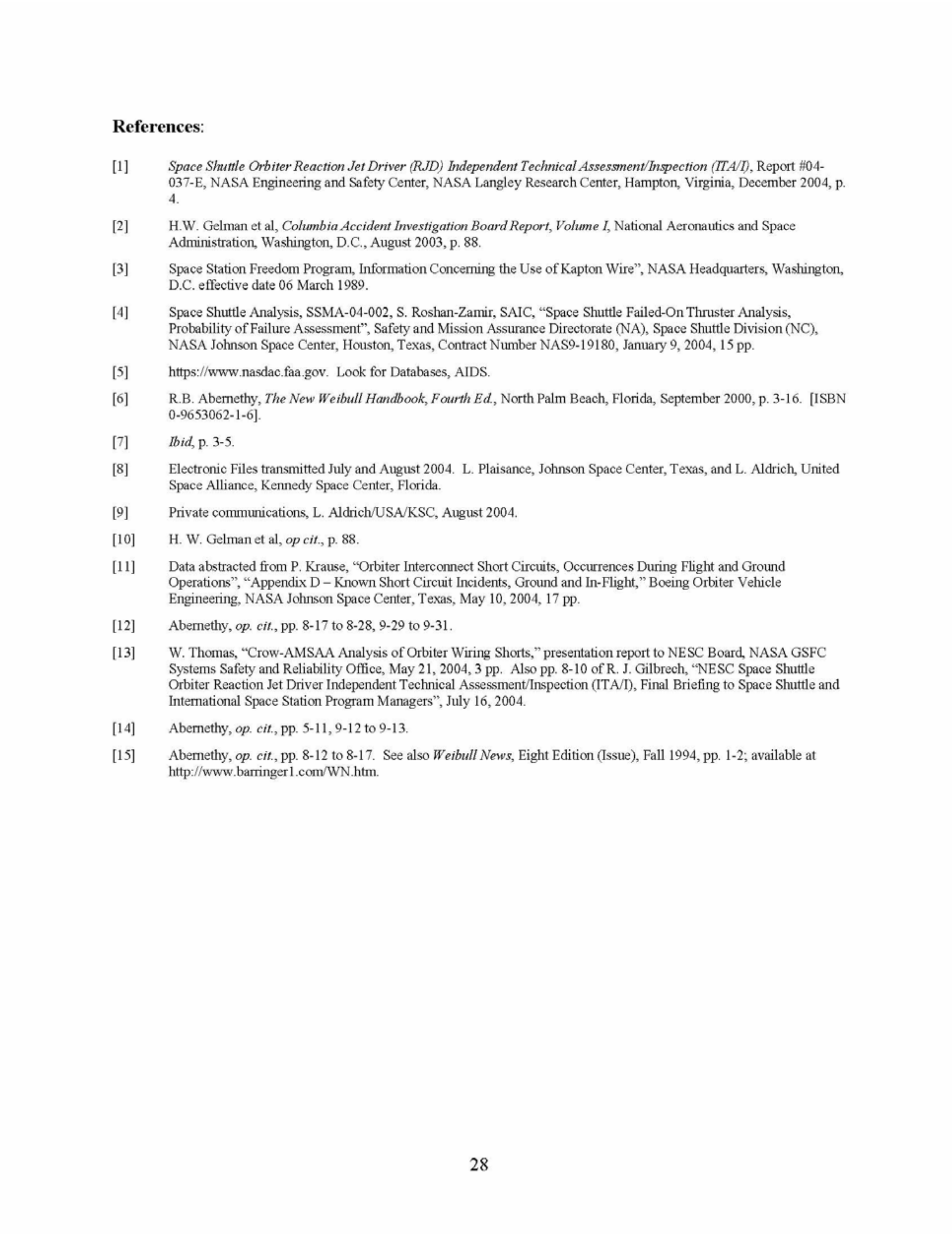


compilation and analyses can be documented to assist the Program in performing these evaluations.

3. Using CA techniques to trend wiring damage data would assist the Program in accurately tracking and assessing the wiring inspection-maintenance process for the other vehicles. The goal would be to get the wiring inspection-maintenance process "stable," so that it exhibits a defined occurrence distribution. Ideally, this distribution would have a CA slope of 1.0 or less, indicating either a static process or one which is improving. There must be a positive correlation between damage events detected and damage events existing. Likely, CA techniques also would benefit the Program in other areas of endeavor.

4. Should the Program choose to accurately track induced damage events, wiring damage inspection-maintenance process revisions likely are needed. The goal would be to positively identify and track damage occurrences caused by "non-natural" events or actions.

5. Wire damage occurrences increased over time for OV-103. Recommendation #2, if implemented, will determine if it also exists in OV-104 and OV-105. If wire degradation exists in all three vehicles, the Program should undertake a risk assessment to determine which wiring is critical to the successful operation of the vehicles. This "at risk" wiring should be closely tracked and monitored to prevent future undesirable events.



References:

[1] *Space Shuttle Orbiter Reaction Jet Driver (RJD) Independent Technical Assessment/Inspection (ITA/I)*, Report #04-037-E, NASA Engineering and Safety Center, NASA Langley Research Center, Hampton, Virginia, December 2004, p. 4.

[2] H.W. Gelman et al, *Columbia Accident Investigation Board Report, Volume I*, National Aeronautics and Space Administration, Washington, D.C., August 2003, p. 88.

[3] Space Station Freedom Program, Information Concerning the Use of Kapton Wire", NASA Headquarters, Washington, D.C. effective date 06 March 1989.

[4] Space Shuttle Analysis, SSMA-04-002, S. Roshan-Zamir, SAIC, "Space Shuttle Failed-On Thruster Analysis, Probability of Failure Assessment", Safety and Mission Assurance Directorate (NA), Space Shuttle Division (NC), NASA Johnson Space Center, Houston, Texas, Contract Number NAS9-19180, January 9, 2004, 15 pp.

[5] https://www.nasdac.faa.gov. Look for Databases, AIDS.

[6] R.B. Abernethy, *The New Weibull Handbook, Fourth Ed.*, North Palm Beach, Florida, September 2000, p. 3-16. [ISBN 0-9653062-1-6].

[7] *Ibid*, p. 3-5.

[8] Electronic Files transmitted July and August 2004. L. Plaisance, Johnson Space Center, Texas, and L. Aldrich, United Space Alliance, Kennedy Space Center, Florida.

[9] Private communications, L. Aldrich/USA/KSC, August 2004.

[10] H. W. Gelman et al, *op cit.*, p. 88.

[11] Data abstracted from P. Krause, "Orbiter Interconnect Short Circuits, Occurrences During Flight and Ground Operations", "Appendix D – Known Short Circuit Incidents, Ground and In-Flight," Boeing Orbiter Vehicle Engineering, NASA Johnson Space Center, Texas, May 10, 2004, 17 pp.

[12] Abernethy, *op. cit.*, pp. 8-17 to 8-28, 9-29 to 9-31.

[13] W. Thomas, "Crow-AMSAA Analysis of Orbiter Wiring Shorts," presentation report to NESC Board, NASA GSFC Systems Safety and Reliability Office, May 21, 2004, 3 pp. Also pp. 8-10 of R. J. Gilbrech, "NESC Space Shuttle Orbiter Reaction Jet Driver Independent Technical Assessment/Inspection (ITA/I), Final Briefing to Space Shuttle and International Space Station Program Managers", July 16, 2004.

[14] Abernethy, *op. cit.*, pp. 5-11, 9-12 to 9-13.

[15] Abernethy, *op. cit.*, pp. 8-12 to 8-17. See also *Weibull News*, Eight Edition (Issue), Fall 1994, pp. 1-2; available at http://www.barringer1.com/WN.htm.

Appendix H

Team Member Biographies

H-1. Dr. Richard Gilbrech (LaRC) - NESC Principal Engineer
H-2. Robert Kichak (GSFC) - NESC Avionics Discipline Expert
H-3. Mitch Davis (GSFC) - Electrical Systems Branch
H-4. Glenn Williams (GRC) - Avionics
H-5. Walter Thomas (GSFC) - Reliability Engineer
H-6. George Slenski (WPAFB) - Principal Technologist Electronic Matls. Eval.
H-7. Mark Hetzel (JPL) - Wiring

H.1 Dr. Richard "Rick" Gilbrech began his career with NASA at the Stennis Space Center (SSC) in 1991 starting in Propulsion Test Technology. He next served as Project Manager for a liquid hydrogen foil bearing turbopump test program. In 1995, he was selected as the SSC X-30 National Aerospace Plane Project Manager responsible for construction, activation and operation of a facility to test actively-cooled structures. In the same year he was also selected as the X-33 Project Manager converting the A-1 test stand at SSC from Space Shuttle Main Engine testing to Linear Aerospike turbopump, single and dual engine testing. He then served as Chief of the Propulsion Test Engineering Directorate from 1998 to 2000 until departing for a six-month detail at Johnson Space Center (JSC) as the technical assistant to the Space Shuttle Program Manager. He returned to SSC and was selected as Deputy Director of Propulsion Test. In 2003, Dr. Gilbrech became Manager of the Program Integration Office responsible for managing NASA's rocket propulsion test facilities located at SSC, Marshall Space Flight Center, JSC's White Sands Test Facility, and Glenn Research Center's Plumbrook Station. He relocated to NASA Langley Research Center in late 2003 to serve as a Principal Engineer for the NASA Engineering and Safety Center (NESC). In December 2004, the NESC selected Dr. Gilbrech as their new Deputy Director. Dr. Gilbrech received a B.S. degree in Aerospace Engineering from Mississippi State University, and his M.S. and Ph.D. degrees in Aeronautics from the California Institute of Technology.

H.2 Mr. Robert Kichak began his career with NASA-GSFC in 1965 as a co-op student from Cleveland State University. After graduation in 1969, he developed various flight DC-to-DC power converters for IMP-I/H/J, RAE-B, OSO-I, IUE, and HEAO-B. From 1977 to 1982, he served on the Multimission Modular Spacecraft (MMS) Project. There, his duties evolved from power subsystem engineer to Manager and Technical Officer for the Modular Power Subsystem for SMM and Landsats 4 & 5, to MMS Flight Support System Integration and Test Manager. In 1982, he was appointed Head of the Payload Interfaces and Instrument Power Section, where he led development of power electronics for COBE instruments and for the Gamma Ray Observatory (GRO) Energetic Gamma Ray Explorer telescope (EGRET) instrument. He served as Head of the Space Power Applications Branch from 1985 to 1992, where he supported the Hubble Space Telescope (HST), GRO, UARS, and GGS. From 1992 to 2001, he served as Associate Chief of the Electrical Engineering Division. Mr. Kichak then served as the Division's Chief Engineer where he chaired or served on several anomaly resolution and technical review teams. Mr. Kichak has one patent and two technical papers, and was awarded the NASA Exceptional Service Medal in 1995 for his contributions in the development of spaceborne power systems. In 2003, he served as an instructor for the space power segment of a satellite design graduate class at the University of Maryland, and was awarded the GSFC Award of Merit. In his current role, Mr. Kichak serves as the NESC Discipline Expert for Power and Avionics.

H.3 Mr. Mitchell Davis has 20 years expertise in electrical and electronic systems, all with NASA GSFC. As GSFC's Branch Chief Engineer, he is recognized as an expert in space flight electronics architecture, space flight electronics design/development/test/validation, and system level electromagnetic compatibility. Mr. Davis provides electrical design and technical guidance for flight projects, spacecraft electrical architectures, grounding concepts, and general electromagnetic compatibility practices for spacecraft. When required, he supports formal engineering boards and participates in nearly 20 GSFC review boards a year. The formal engineering boards include pre-launch anomaly cost/risk assessments as well as on-orbit failure investigations. Recent pre-launch investigation accomplishments include, for example, the SIRTF spacecraft to IRAC electromagnetic interference anomaly discovered only months before launch. As co-chairman, Mr. Davis led the investigation, identified the root cause of the interference and implemented a cost-effective resolution. Project managers frequently request Mr. Davis' expertise in space flight electronics as a consultant, peer reviewer, or as a member of the Code-300 team. Mr. Davis has a B.S. degree in Electrical Engineering (1984) and has received numerous Group Achievement Awards, Performance Awards, and received the NASA Medal for Exceptional Service in June 2003. He has authored/co-authored several technical publications.

H.4 Mr. Glenn L. Williams worked for 18 years as a digital and software engineer before starting a 15-year career at GRC in Code DD, Diagnostics and Data Systems Branch. He spent over 2 years of military time in the Army Signal Corps. After 16 years in industry, Mr. Williams was promoted to Manager of Development at Gould Electronics, Instrument Systems Division in Cleveland, Ohio, a non-defense branch of Gould Electronics Inc. He is a co-inventor on five Gould patents and was the digital engineer on a team receiving a 1980 IR-100 award. After a Gould downsizing in 1989, he brought his Mentor Graphics CAE and digital experience to NASA (Lewis) where he invented the "Video Event Trigger" now patented and licensed to ATM maker Diebold Corp. Mr. Williams has authored several papers on microprocessor and digital signal processing. At GRC in 1989-1992, in addition to getting the Mentor Graphics system running and contributing to the design of circuit boards for the STDCE/USML1 microgravity mission on STS-50, he supported various electronics and Schlieren optics tasks. From 1992-1994, he supported the electrical and optical design of the GRC 270 kilowatt solar simulator. From 1994 to 2003, he supported image processing hardware and "C" software on Combustion Module-1 (STS-83 and STS-94) and later on Combustion Module-2 as Lead Avionics Engineer for CM-2 on Shuttle *Columbia* (STS-107). He worked as Lead Software Engineer on a new microgravity project in the area of spectrophotometry until funding cuts in the spring of 2004. He currently has a new project in biomedical image processing software in MATLAB and C/C++. Mr. Williams is a 2004 recipient of a Silver Snoopy Award for his work on CM-2, including the recovery of data from damaged solid state data recorders. Mr. Williams holds a B.S. in Engineering from the California Institute of Technology and an M.S.E.E. from University of Utah.

H.5 Mr. Walter Thomas has 16 years of industry experience in product and process research, development and engineering, manufacturing, and quality assurance in the glass, electronic component and packaging industries. He has consulted for component suppliers and aerospace manufacturers in glass and ceramic sealing technologies and technical glass applications. He has worked at NASA's GSFC for the past 18 years in the areas of electronic parts, component and packaging engineering and reliability engineering. He has performed and managed reliability engineering tasks (e.g., FMEAs, RBD, predictions, life test assessments, risk assessments) for space flight programs, solved problems, and provided risk assessments for part, component, and systems issues affecting space flight and other programs. His areas of expertise include Weibull and other statistical analyses, field performance evaluations, system modeling, and technical and electronic glass applications. He presently works as a Reliability Engineer in the NASA GSFC Systems Safety and Reliability Office. Mr. Thomas holds a B. Ceramic Engineering from Georgia Institute of Technology and a M.S., Ceramic Engineering, from the University of Illinois.

H.6 **Mr. George A. Slenski** has worked in the area of electronic failure analysis for the United States Air Force since 1980. Since 1990, Mr. Slenski has been the lead engineer in the electronic materials evaluation group that is responsible for planning, organizing, and conducting Air Force electronic failure analysis and materials evaluations on fielded and new systems. He has personally conducted several hundred failure investigations, with many supporting aircraft mishap boards. Mr. Slenski also evaluates state-of-the-art electronic assemblies and provides management with performance and production risk assessments of new technology. Tasks have included performing hardware audits, field investigations, mishap investigations, corrosion surveys, and assessing the materials and manufacturing process capabilities of DOD contractor facilities. Mr. Slenski has managed efforts that have developed new aerospace wire insulations; a handbook for conducting electrically-related mishap investigations, and a program for developing a life prediction system for aging wiring systems. Mr. Slenski is presently the Principal Technologist in the Electronic Materials Evaluation Group in the Air Force Research Laboratory's Materials Directorate. He has co-authored several chapters in failure analysis handbooks related to electronic packaging, wiring, and general failure techniques, has guest lectured on electronic failure analysis techniques, and presented over thirty technical papers. He is also the Air Force representative to the SAE aerospace committees on wire and cable and electrical and electronic distribution systems. Recent activities have included testifying as a wiring expert at the NTSB public hearing on the TWA 800 aircraft accident, member of the 1999 NASA Shuttle Independent Assessment Team that reviewed the space shuttle's overall reliability, technical consultant on the *Columbia* accident board related to electrical systems and a technical contributor to the FAA aging aircraft sub-committee on wiring inspection. Mr. Slenski was the senior DoD technical lead for the White House initiated study entitled "Review of Federal Programs for Wire System Safety". Mr. Slenski's current emphasis area is on characterizing and assessing aging electronic systems, specifically dealing with wiring systems and managing research initiatives to improve wiring system integrity. Mr. Slenski holds a B.S. degree in Electrical Engineering from University of Florida and an M.S. in Materials

Engineering from University of Dayton. Mr. Slenski holds Certificates as a level 2 and 3 DOD Acquisition Official for Science and Engineering.

H.7 **Mr. Mark Hetzel** has worked at the Jet Propulsion Laboratory for over 10 years, currently serving as Group Supervisor for the Cabling Engineering and Mechanical Integration Engineering Groups. He has managed the design and fabrication of numerous spacecraft and instrument harness subsystems and flexprint assemblies, including the Mars Exploration Rover flexprints, Mars '98 and '01 Robotic Arm flexprints, the SIR-C Antenna Cabling Subsystem, and fabrication of the Cassini Wide and Narrow Angle Camera hardware. In addition, he was responsible for the design, fabrication, and proof testing of the SIR-C Antenna lift fixtures and Cassini spacecraft support stand and dollies. He worked for General Dynamics Pomona Division from 1986 to 1991, designing wiring harnesses and EMC test fixtures for Phalanx and Standard Missile. During this time period, he also served as Packaging Engineer for the Standard Missile Environmental Telemeter. Mr. Hetzel holds a B.S.M.E. degree from California State Polytechnic University, Pomona.

Report Approval and Document Revision History

Approved:	Original signed on file	3-22-05
	NESC Director	Date

Version	Description of Revision	Office of Primary Responsibility	Effective Date

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
01- 03 - 2005

2. REPORT TYPE
Technical Memorandum

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
Space Shuttle Orbiter Reaction Jet Driver (RJD)

Independent Technical Assessment/Inspection (ITA/I) Report

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Gilbrech, Richard J.; Kichak, Robert A.; Davis, Mitchell; Williams, Glenn; Thomas, Walter, III; Slenski, George A.; and Hetzel, Mark

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
104-08-46

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NASA Langley Research Center
Hampton, VA 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER
NESC-RP-05-18
L-19119

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)
NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
NASA/TM-2005-213750/Version 1.0

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified - Unlimited
Subject Category 18
Availability: NASA CASI (301) 621-0390

13. SUPPLEMENTARY NOTES
An electronic version can be found at http://ntrs.nasa.gov

14. ABSTRACT

The Space Shuttle Program (SSP) has a zero-fault-tolerant design related to an inadvertent firing of the primary reaction control jets on the Orbiter during mated operations with the International Space Station (ISS). Failure modes identified by the program as a wire-to-wire “smart” short or a Darlington transistor short resulting in a failed-on primary thruster during mated operations with ISS can drive forces that exceed the structural capabilities of the docked Shuttle/ISS structure. The assessment team delivered 17 observations, 6 findings and 15 recommendations to the Space Shuttle Program.

15. SUBJECT TERMS
Darlington transistor; Probabilistic risk assessments; RJD; Pin-to-pin short; Wire short; Switch; Orbiter

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			STI Help Desk (email: help@sti.nasa.gov)
					19b. TELEPHONE NUMBER ***(Include area code)***
U	U	U	UU	160	(301) 621-0390